UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA,

-against-

VITALY KORCHEVSKY and,
VLADISLAV KHALUPSKY

Defendants.
----------x

15-CR-381(RJD)

United States Courthouse
Brooklyn, New York
June 18, 2018
10:00 a.m.

TRANSCRIPT OF CRIMINAL CAUSE FOR TRIAL
BEFORE THE HONORABLE RAYMOND J. DEARIE
UNITED STATES SENIOR DISTRICT JUDGE
BEFORE A JURY

APPEARANCES

For the Government: RICHARD P. DONOGHUE, ESQ.
United States Attorney
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201
BY: RICHARD M. TUCKER, ESQ.
JULIA NESTOR, ESQ.
Assistant United States Attorneys

For Defendant Korchevsky: SULLIVAN BRILL
115 Broadway, 17th Floor
New York, NY 10006
BY: STEVEN G. BRILL, ESQ.
JAMES L. HEALY, ESQ.

RACHEL BRILL, ESQ.
263 Domenech Avenue
San Juan, P.R. 00918

For Defendant Khalupsky: FEDERAL DEFENDERS OF NEW YORK
One Pierrepont Plaza
Brooklyn, NY 11201
BY: MILDRED WHALEN, ESQ.
LaKEYTRIA W. FELDER, ESQ.

Court Reporter: Rivka Teich, CSR, RPR, RMR, FCRR
718-613-2268 RivkaTeich@gmail.com

Proceedings recorded by mechanical stenography. Transcript produced by computer-aided transcription.

(In open court.)

THE COURTROOM DEPUTY: All Rise.

THE COURT: I was out of town over the weekend and I haven't had a chance to study these letters and the attachments that come with them. I certainly have a gist of it. But I have a couple of questions.

First of all, with respect to the forgery of bank accounts, is it not my recollection that Igor finally admitted to doing just that at trial?

MS. WHALEN: Your Honor, I believe that he admitted to forging those bank documents. He did not admit to having sent them to an attorney in Latvia. And the position of the Government that it was some kind of funny business and they were the victims of loses of $150,000, that still stands.

THE COURT: I'm focusing on his trial testimony. I thought he admitted those series of letters of the exact same amounts on different company stationary.

MS. WHALEN: If I could clarify. The documents we showed him were in light of your Honor's ruling that we couldn't bring in extrinsic evidence of the Latvian bank fraud. So what we did is we found these other frauds.

THE COURT: Your Honor, did not rule. His Honor said you could examine that on the Latvian matter on the issue of credibility. All right. You certainly didn't proffer any extrinsic evidence that I precluded. Let's keep the record

clear.

MS. WHALEN: What I'm trying to explain -- our understanding was we weren't permitted to introduce extrinsic evidence. While we were investigating the Latvian documents, we found that fraudulent documents had created and sent to other individuals that happened to be the same, of the same month that the Latvian bank fraud was conducted. I believe that Mr. --

THE COURT: They were different documents than the ones that were the subject of cross-examination.

MS. WHALEN: What they were is, Mr. Dubovoy created false documents for the same month, July 2013, where he altered the numbers. He sent them to a realtor. He then sent an exact copy of those that had been further altered in terms of the account number and the account holder, and sent those to a friend of his, that in the proffer he later acknowledged to the Government was the owner of Everest Construction.

THE COURT: During his trial testimony, which is what my focus is now, he acknowledged that those documents were obviously not legitimate and they were prepared in connection with the Latvian attempt to acquire the hotel.

MS. WHALEN: No, your Honor. I'm sorry. It clearly wasn't clear.

There were three sets of documents that we confronted him with. The first were the actual phony bank

records for July 2013. Those are the bank records that the government in Latvia is claiming were forged. But the copies that we have are the genuine copies, we don't have a copy of the forgery.

The second documents that we showed the witness were forgeries of that same month of bank statements but they were sent to other individuals for other purposes not related to the Latvian bank or the Latvian hotel transfer.

THE COURT: All right. So then he's interviewed and he admits to the Government that he created false documents in connection with the Latvian deal. And the other aspect of it is that he owned additional companies that he did not disclose. And his reasons for not disclosing, he said they had no assets.

As your letter says, he was impeached at trial regarding the forgeries. What else is it that want to do with it? You want to bring out the fact of during the interview on the 16th he admitted that he created false documents?

MS. WHALEN: Your Honor, I think that we --

THE COURT: One at a time, Mr. Brill, please.

MR. BRILL: Of course.

MS. WHALEN: If your Honor is not considering my motion to strike his testimony --

THE COURT: It's rather extraordinary. Motion to strike, much less a motion to preclude. I'm trying to get at

the hub of your --

MS. WHALEN: I guess what I want the Court to do in the absolute minimum is to give a curative instruction.

We've drafted one that would say, "You heard testimony from Igor Dubovoy as a witness for the Government. And I'll instruct you that Mr. Dubovoy has lied and failed to disclose information concerning a number of matters.

"First, Igor Dubovoy falsified dozens of documents on numerous occasions to purchase real estate. This occurred during the time frame of the conspiracy to commit wire fraud and was charged within the District of New Jersey.

"Second, Igor Dubovoy failed to disclose a number of bank accounts on the financial affidavit he completed as part of his cooperation agreement and guilty plea.

"Third, Igor Dubovoy falsified bank records in an attempt to purchase a Latvian hotel in 2013. He provided these false documents to an attorney in Latvia in the attempt to purchase the hotel. Any money he claims to have paid toward this venture should be considered by you to be an effort to complete this crime.

"I will instruct you further at the close of the case on how to consider witnesses who have been impeached. But at this point I instruct you consider any testimony you have heard from Igor Dubovoy with extreme care."

Your Honor, if I could just add a little bit as to

why we think the more extraordinary remedy is required in this case. The reason we think a more extraordinary remedy is required is because it appears the Government did absolutely nothing to follow up on the Latvian bank fraud claim. They presented papers to the Court and to the defense trying to preclude us from cross-examining about this incident. They made it seem that there was no evidence out there, other than the Latvian Government's claim that this fraud had taken place. And that the defense cross-examination on this topic would be considered harassment.

Your Honor, the Government got the Latvian claim in January 2018. They appeared to simply have asked the witnesses about it, and when the witnesses denied it they did nothing further. The Boni bank records, and they are in evidence now as Defendant's exhibit HH, show that on July 3rd, exactly as stated in the Latvian bank account, money was transferred between DBM and Boni.

THE COURT: I read your letter. Now let me ask you a question, is there any authority for this?

MS. WHALEN: Your Honor, the authority I think -- I think, your Honor, the authority is that the Government has presented these witnesses as truthful. I don't have specific authority in this circuit to strike the witness' testimony in its entirety, but given the procedure of the Government in this case to hide a specific incidents of money laundering

dead in the center of this money laundering conspiracy, the efforts that the Government failed to take to follow up, and then the presentation that they made with this witness talking about his cooperation agreement, talking about if he lied it would be taken away, the jury is going to be left, while they recognize there is impeachment, they have been given no further instruction, no further evidence to the extent of how serious this is. How seriously it should be considered.

The Government is then going to present Arkadiy Dubovoy and we believe he has the same problems in his case. They are going to be able to sanitize his testimony. None of us can have any confidence that what he will say is the truth.

Mr. Brill confronted Igor Dubovoy about lying on the stand. And he told us that he wouldn't; but in fact, he didn't disclose all of this.

THE COURT: I have your letter. I'm going to read it more carefully. I'd like to see the proffer instruction. It's rather extraordinary. I've never heard it from the Court. Would I not be usurping the jury's instruction, not to mention your own?

MS. WHALEN: In this instance a fraud is perpetrated on this jury. This witness has been presented as a truthful witness, your Honor. I don't think that can stand. I think the professional --

THE COURT: The Government doesn't boast for the

truthfulnesses for the witnesses, of its witnesses. Their obligation is to put testimony on that they understand is truthful.

MS. WHALEN: But, your Honor, when they go through the cooperation agreement and they go through these enormous penalties that will proceed if this witness is not truthful, and then the witness is shown not to be truthful, the jury needs to be instructed on that.

THE COURT: They are going to be instructed on it, how to consider the testimony of such people. Why isn't this your testimony? Why can't you bring this all out in the normal course of cross-examination?

MS. WHALEN: Are we going to be allowed to bring out the fact that the day after he testified they spoke to him and elicited additional information?

THE COURT: Why not?

MS. WHALEN: We can put that 302 into evidence?

THE COURT: I haven't seen the 302, but why not? Why not bring out the fact that the day, after he admitted that he prepared phony documents. It's all about credibility. I'm not standing in your way on that issue. I'm asking a very simple legal question, is there any precedent for this sort of thing? I've never heard of it, to be honest with you.

MS. WHALEN: I think that Professional Rule of Conduct 3 --

THE COURT: You're accusing the Government -- you're not only accusing the Government of being slipshod of their handling of the Latvian matter, you're accusing the Government of perpetrating a fraud of the Court.

MS. WHALEN: I'm not arguing that the Government is perpetrating a fraud. But that the interview they conducted after the fact makes it clear that Mr. Dubovoy was not transparent in all of his discussions with them. That he lied in his proffers and withheld information. And I think they have an obligation to notify the Court as to that. And I think that since the jury in this case is the tribunal, that the jury needs to be notified as well.

THE COURT: What he admitted to in the interview, in the post-testimony interview, is the essentially what he admitted to during his trial testimony.

MS. WHALEN: He admitted that he had done it dozens of times, not just once, which we didn't know about that, it wasn't presented to the jury.

THE COURT: He did testify -- I have to look at it more carefully, he did testify that he done it over and over again.

MS. WHALEN: I don't believe that he did.

THE COURT: Your colleague brought out a series of letters, one after the other.

MS. WHALEN: Two letters and one actual bank

account -- two e-mails and one actual bank account.

THE COURT: I have more confidence in your recollection than mine.

MS. WHALEN: I don't believe -- it doesn't rise to the dozens of times that he had admitted to the Government.

The second thing that he did not admit is the fact that after he forged the documents he provided them to an attorney in Latvia. The Government on their direct has left an impression that Igor was somehow a victim in this case in losing $150,000; that's not what it is.

THE COURT: For what it's worth, and it's not worth anything, when he left the witness stand I didn't have that impression, but that's a different matter.

Well, I'm sorry, I guess I'm an old-fashioned guy. I want to look at this more carefully. I think my gut tells me the thing to do is bring old Igor back and let you have it at.

MS. WHALEN: No, your Honor. No one can trust that what he says is the truth.

THE COURT: Is that my function?

MS. WHALEN: Judge --

THE COURT: A lot of what he said is the truth, obviously, because both, all sides, brought it out. A lot of what he said is the truth.

MS. WHALEN: Judge, my concern is that when a

witness has perjured himself and when a witness has deliberately withheld information from the Government, putting him back on the stand adds some air of credibility to him, aura of creditability that he's somehow worthy of listening to again. I don't believe that that's appropriate.

If the Court is not going to strike his testimony and the Court is unhappy with my curative instruction, I think that some curative instruction should be given. But recalling him, putting him back on the stand, making it look like he understands his oath to tell the truth, I do not want that remedy, your Honor.

THE COURT: I don't understand. You just summarized in rather impressive fashion all his failings and you want to make sure the jury understands them. Why can't you do that through his testimony his cross-examination?

MS. WHALEN: Is the Government doing to be permitted to redirect him?

THE COURT: What are they going to do?

MS. WHALEN: I don't know, but any attempt to sanitize this is not an acknowledgment of what he's done.

This is a case where there have been millions of dollars transferred from bank accounts and there is no record of where that money has gone. It appears that there are shell companies all over the world that have received these assets. So for these individuals to come in and lie and say, okay,

maybe I do a couple of years in jail but I've got millions to get me through is a real issue in this case.

I think it goes to the fact of whether these people made a calculated business decision as to what they were going to do and what they were going to have after they completed this prosecution. I think it goes to their credibility. I don't think they can be trusted.

THE COURT: It may very well, I'm not arguing that point. What I'm saying is, what are the outer limits of my authority? You haven't given me the authority. In fairness to you, I know you regard this as a serious issue, I want to continue this more carefully. We'll continue the discussion.

I have another matter, and I'll give you time to respond. Another matter that just came up. Ms. Mulqueen told me just before I took the bench that one of the jurors, juror seven, a gentleman with a lengthy hair, salt and pepper, called her this morning -- and Ellie, you'll stop me if I misstate this.

COURTROOM DEPUTY: I will.

THE COURT: Said that he wondered whether or not he could have an opportunity to speak to the judge before trial today. And Ellie probing a little bit said, What is the nature of it? He said, Well, you recall the judge told us not to discuss the case at all. Ellie said, Yes. And he said, Well, I'd like to discuss the case. And she said, Is there

anything you can tell me about it? He paused and said, Well, actually I'm the person who said something in the jury room.

That's it, right, Ellie?

COURTROOM DEPUTY: Correct.

THE COURT: There you have it. I'll give you time to come to contemplate that development. I'm not going to delay the starting trial if everybody is here, but at some point we're going to have to speak to this chap, speak to what he's got. Ellie advised to him not to discuss the case. She asked him, did he understand the instruction, he assured that he did. She told him going forward no further discussions, he said he wouldn't. There you have it.

Let me go back to studying these and we'll continue this discussion later in the day.

I take it Igor is not about to get on a plane for Katmandu or anything of the sort?

MR. TUCKER: Mr. Dubovoy is back in Atlanta, but can be back in New York quickly if needed. If we learn today that he's going to be recalled, he can be back in New York by tomorrow.

THE COURT: I'm not going to make any decisions until I feel I fully consumed this. Relax for a few minutes. I'll be back once we have our jury.

(Brief recess.)

THE COURT: Have a seat. I think what we'll, do

unless you have better thought, is speak to this chap at the break. The question I have for you is, would you prefer that I interview him privately with the reporter of course, or is it your preference that I interview him here in open court?

My personal experience is jurors are a little more forthcoming in the comfort of an office, but I certainly appreciate the fact that you rather see it in live-time his responses. Obviously we would have to follow up and I intend to do that at the break.

One thing we know for sure, I haven't yet completed reviewing these documents. We know for sure if the Government is aware one of its witnesses has given false testimony, it has an obligation to do something about it. With that thought, we'll get underway, to be continued.

MR. TUCKER: Your Honor, should I put my witness on the stand?

THE COURT: I think we may be down a juror. You can bring your witness in.

(Whereupon, the witness resumes the stand.)

THE COURT: The witness, Arkadiy Dubovoy, is he going to need an interpreter?

MS. NESTOR: Yes, your Honor.

(Jury enters.)

THE COURT: Good morning, folks. Please be seated, everyone. Welcome back.

We are ready for our next witness, Mr. Tucker.

MR. TUCKER: Your Honor, this is a continuation of the testimony of Agent Shahrani.

THE COURT: Yes, indeed. I remind the witness having previously been sworn you remain under oath.

THE WITNESS: Yes, your Honor.

(Witness takes the witness stand.)

SAMAD SHAHRANI, called as a witness, having been previously first duly sworn/affirmed, was examined and testified as follows:

MR. TUCKER: May I inquire, your Honor?

THE COURT: Yes, sir.

DIRECT EXAMINATION

BY MR. TUCKER: :

Q Good morning, Agent Shahrani.

A Good morning.

Q Before we ended the day on Thursday you were describing your forensic review of the images of those two computers that were seized in the Ukraine in November 2012; is that right?

A That's correct.

Q Just to orient the jury and the Court, as you testified about image 4A, you'll be referring to 3500SS2, which is before you?

A That's correct.

Q Please remind us, did you see any evidence on image 4A

that that computer had been used to run a program called SQLMap?

A I did.

Q S-Q-L Map; is that right?

A Yes. We pronounce it sequel for convenience, but it's SQL.

Q Before we broke you were explaining SQL. Can you explain what SQLMap is?

A As I said SQL is a language for constructing a database. SQLMap is a tool that is used to map out the structure of databases. It's a hacking tool. Basically it can enumerate a database, so describe the structure, the database, the names. If you think of a database as a Excel spreadsheet, the names, columns, the rows, the individual pages inside of the workbook, for lack of a better term. Then SQLMap can inject commands. So it can interact with the database and try to get data out of the database.

Q Is that technique sometimes called SQL injection?

A It is.

Q What indications on image 4A did you see that that computer had been used to run SQLmap?

A The reverse SQLmap log files.

Q Explain to the jury what a SQLmap log file is?

A Sure. When you're using a variety of programs most of them leave log files. A log file is a record of what an

individual program did. In the case of hacking tools, or penetration tools, things like that usually they will contain data about what the program found, what it was told to do, what it found, then just logs that. The reason you keep those log files is if you didn't have them you wouldn't know what a program did. It would be like asking a question and not listening to the answer. The log files record the answers to the questions that the SQLmap tool received.

Q Do those log files include, among other things, the dates and times that the SQLmap tool is used and information about data that was extracted, if any data was extracted?

A Typically, yes.

Q Did you see indications on image 4A that SQLmap had been used to target the newswire, PR Newswire.

A I did.

Q Please tell the jury what you saw.

A So I believe I'll be referring to page 18.

Q Of 3500?

A Yes, 3500SS2.

Q Tell the jury what you saw.

A So basically there were indications that connections had been made from the SQLmap tool to media.prnewswire.com, amongst other addresses.

Q So it's clear, Agent Shahrani, as you're referring to SS2 did you author that report?

A No, I didn't author this report, but I verified the results.
Q So you personally witnessed the facts in evidence that you're testifying about?
A That's correct.
Q What was the date -- what were the dates associated with the SQLmap sessions targeting the PR Newswire domain?
A So the two, initially it looks like it was May 30 of 2012 and then May 31 of 2012.
Q Did you see any evidence of information or data being downloaded from PR Newswire systems?
A Yes, there were artifacts in Firefox that indicated that specific files had been downloaded.
Q Can explain, what is Firefox?
A So Firefox is the Mozilla web browser. Just like there is a variety of word processing programs, there are a variety of web browsers. There is also Firefox, which is made by Mozilla; people are familiar with Internet Explorer; Chrome which is made by Google, a variety of other flavors.
Q In this instance you saw evidence that Firefox had been used to take data from the PR Newswire domain?
A There was, there had been a download.
Q Did you see indications in those log files that that computer image 4A had been used to target Business Wire using that SQLmap software you just described?

A I did.
Q What did you see?
A On, it looks like, March 16 and March 24 there was indications of connection to R.B2HM.com, which I previously mentioned in the testimony was associated with Business Wire.
Q For the record, Agent Shahrani, March 16 and March 24 of what year?
A Sorry, of 2012.
Q Did you see any other references to the Newswire companies in your review of that image 4A?
A I did.
Q What did you see?
A There were other accesses including Marketwired.
Q Did you review the contents of a folder called trading?
A I did.
Q That folder, trading, was that in that file hierarchy that we looked at on Friday?
A Yes, by default part of the hierarchy.
Q Do you recall what the file above trading was the parent file for trading?

MS. WHALEN: Your Honor, is 3500SS2 in evidence?

THE COURT: I don't believe it is.

MR. TUCKER: I'm not offering it, your Honor. The witness is using it to refresh his recollection.

MS. WHALEN: I think the witness is reading. He's

pointing to pages and going through the documents. If it refreshes his recollection, he can review it and testify to it. I think right now he's reading from a document not in evidence.

THE COURT: Who prepared this document?

THE WITNESS: This document was prepared by Mandiant Corporation.

THE COURT: SS --

MR. TUCKER: 2, your Honor.

THE COURT: 2. And what did you do once you received it?

THE WITNESS: So I received the report, I went through the records that it refers to, and verified that the information was accurate.

THE COURT: I see. I'll hear the objection. How should we proceed?

MR. TUCKER: I can continue to move on. I think the witness -- I think I can continue to move on, your Honor.

THE COURT: You can continue to move on. Why don't you just move on.

MR. TUCKER: I'll move on, your Honor.

THE COURT: But if you're going to refer to the document for any reason let us know. It's apparent at times, but let us know if you need to refer to that document to refresh your recollection.

THE WITNESS: Yes, your Honor.

THE COURT: Go ahead, sir.

BY MR. TUCKER: :

Q Agent Shahrani, you testified a moment ago that you saw folders that referred to the different news wires from your own personal review?

A That's correct.

Q Tell the jury what you saw.

A So basically, like I said, the folders contained names after a specific directory, the directories structures reflected the names of sites that had been accessed.

Q Agent Shahrani, did you personally take your own notes about those different folders found in image 4A?

A I did.

Q Is that 3500SS7 that's before you?

A I did.

MR. TUCKER: The witness will refer to that in the course of his testimony, with the Court's permission?

THE COURT: That's your notes?

THE WITNESS: Yes, your Honor.

THE COURT: In the process of verifying the information?

THE WITNESS: That's correct, your Honor.

THE COURT: SS7. Let's us know if you're going to refer to it.

MR. TUCKER: Thank you, your Honor.

Just for the witness, Ms. Mulqueen?

COURTROOM DEPUTY: Certainly.

MR. TUCKER: Showing the witness what is marked for identification as Government's Exhibit 408.

COURTROOM DEPUTY: 408?

MR. TUCKER: Correct, and 409.

BY MR. TUCKER: :

Q Do you recognize those documents?

A I do.

Q Where did you find them?

A They were found in a directory Business Wire.com and they appear to be output of SQLmap and other tools being run.

Q So it's clear, that was the Business Wire.com folder on image 4A?

A That's correct.

Q Printouts of files?

A These are copies of text files that were on the system.

Q Did you review 408 and 409 prior to your testimony today?

A I did.

Q Are they fair and accurate copies of two of the files found in that Business Wire.com folder?

A Yes.

MR. TUCKER: The Government moves 408 and 409 in evidence.

THE COURT: Any objection?

MR. HEALY: No objection, your Honor.

THE COURT: Received 408 and 409.

(Government Exhibit 408 & 409, was received in evidence.)

MR. TUCKER: May we publish?

THE COURT: Go ahead.

BY MR. TUCKER:

Q Look at 408, Agent Shahrani, can you tell us what is the title of this file?

A The file is hack.txt.

Q So it's clear, did you name this file hack.txt?

A No, that's the file in the system.

Q So this is the name of the file as saved in that Business Wire.com folder on image 4A?

A Yes.

Q What is this document, generally, now that the jury can see it?

A As I mentioned early, one of the purposes of SQLmap was to enumerate a database, that's basically what this is, as you can see. It lists the available databases then the structure of it. So the databases of Business Wire own, then it lists out the tables. If you think of, like I said, the database, then there are a number of tables inside of it. Those tables contain information and you can reference that data using SQL

commands.

Q Certain of the data in Government's Exhibit 408, does that out from a program like SQLmap?

A Yes.

Q Now are there also references in this document to what appear to be Business Wire user login credentials and passwords?

A There are.

Q Turning to page six of 408 -- page 9, first. Can I ask you to read this text, please, that I'm highlighting in my copy.

A Operator:X1CK2lgb8KvVg:nextphazenew.

Q Showing you what is in evidence now as Government's Exhibit 409. Directing your attention to this text here, what is this text here?

A It says admins.

Q What is an admins?

A Typically admin is a abbreviation for administrator. Administrator is someone who has high-level access to a computer system or to a computer network.

Q There are a number of names then at Business Wire.com based on the formatting of the different names, what are those?

A It appears to be e-mail address or login then followed by a colon, then a looks like a password. For the last four

there, the long alphanumeric stream, that could be different kind of identifier, but the end of it thereafter the last colon does appear to be passwords.

Q Also directing your attention to the top, what does it say here?

A It says from the Business Wire.com site, it says then create password page.

Q Read this highlighted page.

A Old pass singsing, with no spaces. The new pass is singsing333!.

Q Agent Shahrani, in your -- I'm going to show the witness, and just the witness, what is marked for identification as Government's Exhibit 411 and 444. Do you see those, agent Shahrani?

A I do.

Q What are those?

A Those are output from the Marketwired.com directory.

Q So it's clear, are those files that you found in a folder called Marketwired.com on image 4A?

A That's correct.

Q Are they fair and accurate copies of those specific files that you found on there?

A These are pronounced of text files.

MR. TUCKER: The Government moves 411 and 444 into evidence.

THE COURT: Any objection?

MR. HEALY: No objection.

MS. WHALEN: No objection.

THE COURT: Received.

(Government Exhibit 411 & 444, was received in evidence.)

MR. TUCKER: May we publish, your Honor?

THE COURT: Yes, sir.

BY MR. TUCKER:

Q Now that the jury can see, what was the name of this file in evidence, 411?

A FTP_users.text.

Q What is FTP?

A The file transfer protocol, a long-standing method for transmitting files from one system to another on the Internet.

Q Agent Shahrani, I neglected to clarify this. I'm going to show what you is in evidence as 409, what is the file name of this second document that was found in the Business Wire.com file?

A Hack2.txt.

Q So you found hack and hack2.txt in that Business Wire folder?

A That's correct.

Q Back to Government's Exhibit 411. This was again found in the Marketwired document folder on 4A?

A Correct.
Q Directing your attention here to this first series of digits, what is that?
A That is an IP address and IPv4. There are two kinds of IP addresses out there. This is the more common version that people see. There is also a longer version, IPv6.
Q What is an IP address?
A IP address is Internet protocol address. Everything that connects to the Internet has to have an address so you send data to and from it. There are a lot of different ways to think of it, like a mailbox or a phone number. And basically when a device is connected to the Internet, it says this is my IP address, if you need to send me data, send data to me at this address. Then when you send a query to a website, the server knows where to send the data back to.

Also so you can talk to the servers. We all do things by Google.com. But when you type that in, your computer doesn't actually go to Google.com, it doesn't go to the word Google.com. It looks up the IP address then it goes to that. A lot of this happens behind the scenes.
Q Agent Shahrani, after that IP address you testified about, appear the words distribution:passw0rd, but the zero in the word password is a zero; is that right?
A Yes.
Q Did you see a number of other entries that appear to be

passwords?
A Yes. As you look through this you can see a number of different, whether combinations of usernames and passwords, some of them are very similar, indicating maybe there was an iteration. Like people typically, when they are forced to change their password, it's fairly common to make finer changes to the password.
Q You saw a references to Marketwired as well?
A That's correct.
Q Showing what you is in evidence as Government's Exhibit 444. What is the title of this file, Agent Shahrani?
A The title is employees.txt.
Q The same file name that you found in that Marketwired.com file on image 4A?
A That's correct.
Q This document includes references to e-mail addresses associated with Marketwired; is that right?
A That's correct.
Q Does it also include what looks to be passwords: changeme and Aloha28?
A A collection of e-mail addresses or usernames and potentially phone numbers, then what appear to be passwords.
Q For the record, Agent Shahrani, this is a 14-page document; is that right?
A I believe so, yes, there are hundreds of records.

Q So fair to say this is just a sample of login credentials and user IDs associated with the different newswires?
A Yes. It depends on the size of the company. Without knowing how many employees or how many accounts are set up, it's at least a portion and potentially all of them.
Q This is a sample of the documents you found on image 4A?
A Yes.
Q There were others?
A Yes.
MR. TUCKER: Ms. Mulqueen, for just the witness.
COURTROOM DEPUTY: Just the witness.
Q What is marked for identification as Government's Exhibit 413, do you recognize this document?
A Yes, I do.
Q What is this document?
A This is from the PR Newswire directory.
Q There was a PR Newswire image on 4A?
A Yes.
Q There were directories on PR Newswire.com, Business Wire.com and Marketwired.com?
A Yes.
Q Is it a fair and accurate copy of one of those files in PR Newswire.com's directory?
A Yes.
MR. TUCKER: We move 413 into evidence.

THE COURT: Any objection?

MR. HEALY: No objection.

MS. WHALEN: No objection.

THE COURT: It is received.

(Government Exhibit 413, was received in evidence.)

MR. TUCKER: May we publish it?

THE COURT: Yes.

BY MR. TUCKER:

Q So now that the jury can see what is in evidence as Government's Exhibit 413, what is the title of this file?

A So the title is SSH_passwords.txt.

Q What is SSH agent Shahrani?

A SSH is the secure show. When you're using a command line interface, like commonly it's a secure way of logging into a server. So if you're SSHing into this, say if you're SSHing into a server, you're connecting to the server, if you're making an SSH connection you're, unless it's a tech company for instance, it's usually a pretty high-level user, usually it's an administrator to the server.

Q If a person has SSH login credentials, to what extent to could they potentially access to the system?

A Depending on whose SSH credentials, they could have anywhere from guest access all the way up to administrative privileges and the ability to do whatever they wanted.

Q This last entry is Jwatkins: it looks like h4ppyj0y, the

A is a four, and the O is a zero; is that right?
A Yes, with an exclamation point at the end.
Q Thank you.
MR. TUCKER: Just for the witness, Ms. Mulqueen.
COURTROOM DEPUTY: For the witness only.
Q Showing the witness what is marked for identification Government's Exhibit 407T, do you recognize this document, Agent Shahrani?
A I do.
Q What is it?
A This is a transcript of Skype messages that's been translated that were located on item 4A.
Q First after all, what is Skype?
A Skype is a chat tool. It can be used both for -- more commonly people think of it as a video conferencing tool, but it has a text chat feature as well. Originally I believe it was an independent company but was bought by Microsoft years ago. Skype and Skype for business.
Q You said this came from image 4A?
A That's correct.
Q Are the chats set forth here in the chat message column and the other associated data to the left and in the column chat ID a fair and accurate copy of the Skype log from that image 4A?
A Yes.

Q There is also a column that says translation, was that on the original computer?
A No, I believe that was done by the FBI.
Q So it's clear, Agent Shahrani, is this each and every Skype message that you observed on image 4A?
A No, this is just a sampling.
MR. TUCKER: We move to admit 407T.
THE COURT: Any objection?
MR. HEALY: No objection.
MS. WHALEN: No, your Honor.
THE COURT: Received in evidence.
(Government Exhibit 407T, was received in evidence.)
MR. TUCKER: May I publish?
Q Now that the jury can see, this is a log of chat messages or exchanges from image 4A?
A That's correct.
Q Based on your review of this particular log of Skype messages, were you able to identify which username was associated with the actual user of image 4A?
A Yes.
Q What was that?
A Vaiobro, V-A-I-O-B-R-O
Q What is Vaiobro?
A Vaiobro is a brand name for Sony computer series. VAIO is commonly laptops, I believe they may also have a desktop

line as well.

Q Agent Shahrani, have you reviewed the contents of 407T?

A I have.

Q Generally, in these Skype messages did you observe discussions about computer hacking specifically hacking the newswire companies?

A I did.

Q I'm going to ask you to read a few portions of this document. Could you read this first message that appears on 407T on the first page?

A From Vaiobro. It says, forward the lists to me. I'm curious.

Q That was sent on June 19, 2012; is that right?

A That's correct.

Q According to the logs?

A Right, that's according to the log.

Q Would you continue reading this next message, please?

A Also from Vaiobro, since I'm not aware of anything of importance except for Business Wire/PRnewswire/Marketwired/Globenewswire.

That's with slashes between each of the companies.

Q Is Globenewswire another news company like Business Wire, PRnewsire and Marketwired?

A It is.

Q On to the second page of 407T, would you read this

highlighted text also from June 19, 2012?

A Utkatra, we'll called that Utkatra, says, is there really a chance to hack them?

Then Vaiobro says, PR or globe are a possibility. Business Wire has been shut.

Q Third page of Government's Exhibit 407T, this is a message that was sent on June 26, 2012; is that right, this last message?

A Yes.

Q I'm going to start here at the end of page two, read that highlighted text?

A This is from Vaiobro. It says, I'm trying to restore PR Newswire.

Q Then there is a pasted additional discussion into that message?

A Yes, it appears to be somebody copy and pasted one message into another.

Q Read for the record the portions of text that I'm highlighting Agent Shahrani?

A This is again from Vaiobro. It says -- this was copy/pasted from the hackerM, didn't you hack Globenewswire.com and Business Wire.com?

Then a subsequent message, hello. I need access to the database or the editorial of Globenewswire.com, Business Wire.com, payout one link for 40K, next one is 100K plus

interest further on or a large one-time lump sum. So is it just those two sites that are of interest? Basically yes.

Q Now turning your attention -- that was sent on 8/3/12, correct?

A Yes.

Q Turning to this next message from 9/8/2012, September 8, 2012, can you read that?

A From Vaiobro, wouldn't you like to finish up Business Wire PR Newswire? If it holds on, then it's possible we can make 200-300K every season.

Q Moving on to the fourth page of 407T, turning to a message that was sent on October 10, 2012, who sent this message?

A This is Vaiobro again.

Q The image of user 4A?

A Yes.

Q Read that.

A As to PR, I got several e-mail addresses of their staffers. I'm hacking their hosting right now.

Q Can you read the next entry here?

A There is a number of shells as well as SQL data inside the hosting.

Q On that same date Vaiobro received a message, what are you busy with; is that right?

A Yes, from user Eminazazov.

Q How do Vaiobro respond?
A Vaiobro says, hacking PR Newswire.com.
Q So it's clear, Agent Shahrani, the majority of these messages that you were reading they were originally not in English?
A It appears to be Cyrillic, I'm not sure what specific dialect.
Q Page seven of 19, I'm going to ask you to read these from October 12, 2012, that I'm highlighting for you now, who sent these messages?
A Again these are from Vaiobro. The messages is, PR Newswire, a pal of mine came to see me today. He said he had already made around 30K before the reporting season starts. It's regarding Marketwired, with PR Newswire can you make ten times that much.
Q Moving on to nine of 19, Government's Exhibit 407T. This is a message from October 17, 2012, Jackpot_1721; is that right?
A That's correct.
Q Read the highlighted text here, again the translation in is English?
A Now is there an opportunity to search through the tickers as the news appears one to two days before, but the admin panel does not retain it so it leaves.
Q How does Vaiobro respond on that same date?

A Vaiobro says, I have already shown you how to look for it.

Q Turning your attention to page 12 of 407T, this is a message on October 26, 2012. Vaiobro, could you read the highlighted text for the record?

A It says, I got the new name for the PRN group and the key for the group. I'm only missing a user account.

Q I want to turn your attention to image 6B, that was the other image that you examined; is that right?

A That's correct.

Q What kind of operating system was 6B running?

A Windows 7 personal computer.

Q Did that particular computer have a name?

A Yes, it's called war, W-A-R.

Q Did you find any tools that you would associate with hacking or penetration testing on that computer?

A I did.

Q Did those tools include SQLmap?

A They did.

Q Did you see any SQLmap log files on image 6B?

A There were.

Q Were any associated with Business Wire domains?

A Yes.

Q Tell the jury.

A If can I refer to the notes here?

Q So Agent Shahrani, for the record are you referring to 3500SS3?
A Yes.
Q Did you author that report?
A No.
Q What is that report?
A A Mandiant report that was commissioned I believe by the Secret Service to look into these drives. Then I went through and verified the contents of what I'm going to speak about.
Q Turning your attention to Business Wire, did you see any SQLmap log files associated with Business Wire?
A I did.
Q What were the dates of those files?
A There were a number of files basically beginning on March 19, 2012, moving all the way through to dates around the 31st, March 31, 2012.
Q I neglected to ask you, Agent Shahrani, on 6B, on your forensic review, were you able to determine the period of time that computer was in use?
A Yes, the last system activity for this device was October late, October 2012, I think the 19th.
Q Did you also see SQLmap log files associated with Marketwired domains?
A Yes.
Q What were the dates of those log wires creations?

A I'll just refer to this.
Q So SS3?
A Yes, this is SS3. You're saying Marketwired?
Q Yes.
A So for Marketwired there is logs, a number of logs here, Marketwired looks like it begins around May 2, 2012.
Q So it's clear, Agent Shahrani, when you're seeing log files and associated dates, what is the significant of those dates?
A Typically with those dates it's saying that's the date, that the day on the computer system that the logs were generated.
Q Does that mean based on that analysis, that was the date that the program was run, that SQLmap was run?
A Assuming that the date on the computer is correct, right, because the system draws this from the computer's date, then that would be the date that these files were, these SQLmap commands, were run, then these files were created as a result of SQLmap.
Q Does you see evidence of data being extracted using SQLmap?
A Yes.
MR. TUCKER: Just for the witness.
COURTROOM DEPUTY: Just the witness.
Q Showing the witness what is marked for identification

Government's Exhibit 427, do you recognize this document, agent Shahrani?

A I do.

Q What is it generally?

A It's a file called employee.CSV, Common Separated Values. So typically if you are copying data out of a database, not from one database to another database, but just to kind of have it as a human readable format, it's export data is a Common Separate Value file. If you look at this in a text file you basically see all the data you're seeing here, but delineated by columns separating it out.

Q Is this document a fair and accurate copy of that file employee.CSV that you found -- withdrawn.

Where did you find this particular image?

A This was found on the work computer.

Q Image 6b?

A Correct.

(Continued on next page.)

DIRECT EXAMINATION

BY MR. TUCKER::

Q Is this is a fair and accurate copy, if you were to print it out, of the document that you found on that war computer in image 6B?

A Yes. To get this kind of layout you'd have to load into something like Excel or some viewer that would display it properly, but, yes, this is a fair and accurate copy.

Q The data that it contains is the same.

A It should be, yes.

MR. TUCKER: Your Honor, the government moves to admit Government Exhibit 427.

THE COURT: Any objection.

MR. HEALY: No objection.

MS. WHALEN: No objection.

THE COURT: 427 received.

(Government Exhibit 427, was received in evidence.)

MR. TUCKER: May we publish?

THE COURT: Go ahead.

(Exhibit published.)

BY MR. TUCKER::

Q I'll zoom in here a little bit, Agent Shahrani. So one of these columns is called email; is that right? I'm trying to highlight it here.

A I think it's EM_email. It's hard to read.

Q Zoom in even more here.
A EM_email, yes.
Q Among the entries in that column are there references to a market wire domain?
A Yes, there are several.
Q Did you also see associated employee information and passwords for those entries?
A Yes. There is a variety of information stored, but if you move there's a field called EM_password, and then also other fields EM_name, underscore first -- underscore name -- excuse me. EM_name_first and then another field called EM_name_last.
Q And, again, this was data that you extracted from image 6B, that computer called war; is that right?
A That's correct.
Q Did you observe any documents that appeared to be press releases, specifically market wire press releases on image 6B?
A I did.
Q How many approximately?
A Dozens.
Q I'm showing you what's been marked for identification, just for the witness, Ms. Mulqueen.
THE COURTROOM DEPUTY: Just for the witness.
Q As Government Exhibit 405.
THE COURTROOM DEPUTY: 405.

BY MR. TUCKER::

Q Is this one of those documents that appear to be a press release?

A It is.

Q And again, where did you find this?

A This was found on the war system.

Q That's image 6B?

A Correct.

Q Is that a fair and accurate copy of the files extracted from image 6B?

A Yes.

MR. TUCKER: Your Honor, the government moves to admit Government Exhibit 405 into evidence.

THE COURT: 405. Any objection?

MR. HEALY: No objection.

MS. WHALEN: No, Your Honor.

THE COURT: Received.

(Government Exhibit 405, was received in evidence.)

MR. TUCKER: May we publish, Your Honor?

THE COURT: Yes.

(Exhibit published.)

BY MR. TUCKER::

Q Agent Shahrani, you testified this was one of dozens press releases from image 6B; is that right?

A Yes.

Q What's the headline here?
A TIBCO software reports Q2 non-GAAP, which is an accounting term, EPS grows 24 percent to 26 cents.
Q Agent Shahrani, at the bottom of this document there is some text, what is that?
A Right. So that's the file name.
Q This was the file name of this particular document as extracted from image 6B?
A That's correct.
Q Now, Agent Shahrani, the press releases that you observed on image 6B, in what format were they stored?
A Most of them were in .rar files.
Q Is that .R-A-R?
A Right.
Q What's the .rar file?
A So it's kind of a running theme, it's yet another format. So in this case it's most similar to what people probably are familiar with as zip files. It's a compressed file format. So there are, again, of variety of different compression algorithms that can be used, they generate a variety of different file names, some are better at compressing say video, others are better at compressing text or other content. In this case the person chose to make it a .rar file. I don't know why but it's a fairly common compression algorithm.
Q Are you familiar with a program call WinZip?

A I am.
Q Could WinZip be used to unpack or unzip a .rar file?
A Certainly.
Q I'm going to show you what's in evidence as Government Exhibit 323.

Agent Shahrani, I'm going to direct your attention here to this icon that appears in the bottom of the system tray. Is that icon familiar to you?

A Yes, it appears to be the WinZip icon for Windows.
Q So it's clear, this WinZip icon could be used to open a .rar file; is that right?
A Sure. That icon suggests that WinZip is open on that computer and then that program would be able to create or open a .rar file.
Q Agent Shahrani, did you see any chat logs on that image 6B, the war computer?
A I did.

MR. TUCKER: Just for the witness, Ms. Mulqueen.

THE COURTROOM DEPUTY: Witness only.

BY MR. TUCKER::
Q I'm showing the witness what's been marked for identification as Government Exhibit 406T.

Do you recognize that document Agent Shahrani?

A I do.
Q What is it generally?

A So these are excerpts of chat logs. You can see timestamp sender, and the original it's written in Cyrillic alphabet, and then the translation into English is on the far right.

Q Are these fair and accurate copies of excerpts of chat logs that you personally observed on image 6B?

A Yes.

MR. TUCKER: Your Honor, the government moves to admit Government Exhibit 406T in evidence.

THE COURT: 406T, any objection?

MR. HEALY: No objection.

MS. WHALEN: No, Your Honor.

THE COURT: Thank you, Counsel. Received.

(Government Exhibit 406T, was received in evidence.)

MR. TUCKER: May we publish, Your Honor?

THE COURT: You may.

MR. TUCKER: Thank you.

(Exhibit published.)

THE WITNESS: Yes.

Q Agent Shahrani, so the jury can see what you were starting to explain, this is the timestamps for the different chats.

A Correct, as recorded by the chat file.

Q This wasn't Skype, right?

A No, this was not Skype.

Q This was a different chat platform?
A Correct.
Q I'm going to turn your attention to certain excerpts here.
On the second page of this document, would you read the highlighted text here, the English translation, Agent Shahrani?
A Sure. It says HTTP://glomosome, so G-L-O-M-O-S-O-M-E.Business Wire.com and then a slash question mark ID equals eight. It says: Got this one. Here is the admin.
And then the same HTTP://glomosome.Business Wire.com/admin/index.php. It says: It's on the secure server no, but still plus something else.
Q That message, that series of messages were sent on February 27th, 2012?
A Yes.
Q And, by the way, so it's clear, Agent Shahrani, these entries say to and from and the username here is N dash dash dash; is that right?
A Yes.
Q That N dash dash dash, that was the user of 6B, according to these logs?
A According to the logs.
Q Turning your attention to the fourth page of 406T. I'm

going to ask you read these series of messages from March 27th, 2012. I'm going to highlight the text here, Agent Shahrani, just bear with me for a moment.

Would you read that text for the jury, please.

A When you get back here write to me right away, there are several problems. The first and largest is that PR is fucked up. They detected the module and removed all our shit there. They took away that temporary server. I haven't gone on to the new one yet, I'm waiting. This happened on the 13th.

The second problem, your guys were detected, they were trading with very big money and there was a lot of fuss about them, about how it's not the season and when it was the season they traded.

Q Again, those messages were sent from the user of 6B on March 27th, 2012?

A Correct.

Q Turning your attention to the next page, there are a series of messages to the user of 6B on that same date. Would you read the highlighted text, please, for the jury.

A Sure. It says: And find out and also that shell there see about raising privileges. Also there is an admin account for biz on the main site.

Q Agent Shahrani, did you see any forensic evidence that that image 6B, that computer 6B had connectivity to the IP address 94.100.218.42?

A I did.
Q We'll refer to that as the 42 IP address going forward?
A Okay.
Q What did you see?
A There were logs and records that were recovered from the system that indicated or that had that IP address present in them.
Q If I could just show the witness --
THE COURTROOM DEPUTY: Witness only.
Q -- what have been marked for identification as Government Exhibits, I'm going to show you a series, Agent Shahrani, 435, 431, 432, 433, and 434.
A Okay.
Q Do you recognize these documents generally, Agent Shahrani?
A I do.
Q Are these fair and accurate copies of files that you extracted from image 6B?
A They are.
MR. TUCKER: Your Honor, the government --
THE COURT: I didn't hear the very last part of your question from image?
MR. TUCKER: 6B, Your Honor.
THE COURT: 6B.
MR. TUCKER: I apologize.

A Yes, they are.

MR. TUCKER: Your Honor, the government moves to admit Government's Exhibits 432, 433, 434, and 435 into evidence.

THE COURT: Not 431?

MR. TUCKER: And 431, Your Honor. Thank you.

THE COURT: Any objection?

MR. HEALY: No objection.

MS. WHALEN: No objection.

THE COURT: They are received.

(Government Exhibit 431, 432, 433, 434, and 435, were received in evidence.)

MR. TUCKER: Thank you, Your Honor. May we publish?

THE COURT: Go ahead.

(Exhibit published.)

Q Turning your attention to what's now in evidence as 435, Government Exhibit 435.

A All right.

Q You testified that there is evidence linking image 6B to the IP address 9410218.42; is that right?

A That's correct.

Q I'm highlighting that particular IP address there. Is that right, Agent Shahrani?

A Yes, that's correct.

Q This came from a file called Exploit; is that right?

A That's correct.
Q Please explain to the jury the significance of the IP address appearing here in Government's Exhibit 435?
A So that address appearing there it says the L Host, which is the local host. This output is from a tool called Metasploit, M-E-T-A-S-P-L-O-I-T, all one word. From -- actually I think the Armitage front-end, like the graphical image interface. And that's Armitage, A-R-M-I-T-A-G-E, I believe.

So basically the system is configured to use that as the local address.
Q Let's take a step back. First of all, what is Metasploit?
A Metasploit is one of the probably most popular, if not the most popular, penetration testing/hacking tool that's out there. It's -- the reason it's called Metasploit is it basically has just a huge variety a meta, a variety of exploits, hence the name Metasploit that can be used to attack a number of different systems in a number of different ways. So it's kind of like Swiss Army knife. It's got a variety of different tools you can use. It can do port scanning, which is basically mapping out computers, it can then find an vulnerability, like identifying systems that have vulnerability, then exploit the system and then provide reports.

Q So is Metasploit like SQLmap in that it can be a penetration testing tool?
A Yeah. Like SQL map is much more limited in terms of just kind of focusing on SQL databases, whereas Metasploit can target a much broad array of targets.
Q So is this information, among other things, log data associated with the use of that Metasploit tool?
A It is.
Q And that again is from image 6B?
A That's correct.
Q Now, please explain what it means, what this particular entry means Set L Host with that 42 IP address.
A Right. So basically you're saying that's the local host. The data should be coming back or you should be communicating with that host. That is the -- when the Metasploit is running when it's going out, there might be a remote host, a target, but then it should be communicating back to the local host. Now that may not necessarily be the computer, the attacker's computer it might be a computer that they control like a different server, but they're basically saying I control this or this is an IP address that you should be talking back to.
Q Right. So let me ask you a couple of questions about that. First, is the local host chosen by the user of that Metasploit software?
A Yeah, that's something that you set.

Q You were explaining a moment ago that this may not be a true IP; is that right?
A Not necessarily -- it doesn't -- I'm sorry, semantics. So it is a true IP, but it may not necessarily be the attacker's home or the IP address where they physically are. In some cases you will run a tool like this and you'll have it communicate it right back to you, right? If I'm the administrator of the system or perhaps not a very good hacker, you might have it send the data right back to you, but that's traceable, right. So in a lot of cases you will set the system up so there's some level of deniability, this is what we refer to as a proxy, so there is basically someone between you. Instead of me walking into the store and stealing something and handing it right over to the person that had me steal it, I use a cutout. There is a server or one or more servers between them and me.
Q So that allows the user to conceal their actual IP address?
A Yes.
Q By the way, Agent Shahrani, when you use a hotspot, a mobile hotspot do you get an IP address assigned when you turn on a hotspot?
A Yes, normally, like I said earlier, if you're connecting to the Internet with any kind of device, your device has to have an IP address, there may be several IP addresses between

it. If you're using a hotspot, typically you're getting assigned an IP address from whatever cellular tower or communication system you're talking to.

Q So that IP address would be different from, say, one's home IP if they were logging in through, you know, a usual cable modem or something like that?

A Sure. If you have an IP address, like I said, these IP addresses are assigned by whoever is giving you Internet access. So if your Internet access is from your home cable system, that's going to be one IP address, but then if you use, say, your cell phone, not connected to your wireless at the house, you just use your cell phone on Verizon or whatever network to go to a different -- or if you go to a web page, even though you're physically at your house, those two different devices, your home computer and your phone would have two different addresses.

Q Agent Shahrani, did you also see evidence linking that image 6B to the email address warninggp@gmail.com?

A I did.

Q I'm going show you first what's in evidence now as Government's Exhibit 431. Again, this was a file that you found on image 6B?

A Yes, but I should note that here it's called gitconfig.txt, so that it's readable, right? We had to make some minor file name changes. On the system it was actually

called .gitconfig, but the content is the same.

Q The point of putting it into a text file was so it could be printed and marked as an exhibit?

A Yes. Basically the way the system was configured before, if you don't change the extension in Windows like that typically it doesn't recognize that as a text file.

Q The email address here, just for the record?

A The email address is warning, W-A-R-N-I-N-G, and the letter G and the letter P @gmail.com.

Q What is git or github, Agent Shahrani?

A So git is hard to explain. So when you're working on software, just like -- when you're working on software you need to be able to keep track of how many different versions of a piece of software you have, right? You're changing the code. Some of those -- so sometimes if it's just you, it's not really hard to do what's called version control, right? I'm the only working on it so it's easy for me to track and I remember what I did yesterday, I remember what I did two days ago, no big deal. If you're working with two or more people, or let's say you're a company like Microsoft and you've got thousands of people working on a piece of code, you need to have what's called a code management system and git is basically that. It's a open source freeware kind of system that you can use to basically manage your software.

So you will have a username, you can set up a

username for it, you can log into it, so if I make a change you can track it. So if you set up git, you create what's called a repo, a repository, and I apologize for the names, I don't make them up, this is industry standard so, so you make a repository and then into that repository people can make push and pull requests so they can basically say, okay, I want to check out a copy of this data, make some changes and then I can put my changes back in. It's basically just a software development and tracking platform.

Q So just to be clear, would you associate the use of git with individuals who have some experience and expertise in writing computer code?

A Yeah, it's especially recently. I mean it's an industry standard now, like git is a pretty common tool, but, yeah, it's not something that the average person would use. It's something that people that are programmers or have some familiarity with programming languages would be interested in. It's not of much use to anybody else.

Q Showing you what's in evidence as Government Exhibit 432. This file is called TheLog; is that right?

A Yes, here it's called TheLog. I think -- yeah, I think it was originally called TheLog.txt as well.

Q And what is it?

A It's just -- it's a log file like a github log file.

Q It's associated with github, right --

A Yes.
Q -- what you were just describing?
A Yes. Just so I'm clear. There's two separate things. There's git, and then there's github, which is -- which uses git. So github is like a website that kind of lets a lot of these repositories talk to each other. You can have a git repository that doesn't use github, but lots of people use github because it lets you trade code back and forth, right? If you're a programmer there's a better than average chance that somebody's already solved a problem that you're looking at and so you can go to github, take a piece of somebody's code, use it in your project if you needed to.
Q Turning to your attention to page 11 of that document, is there a reference in this github log to that email address you were testifying about earlier, warninggp@gmail.com?
A There is, yeah. You can see basically in the log here where the user.email value -- user.email.value was set to warninggp@gmail.com.
Q Showing you what's in evidence as Government Exhibit 433. This was a file called License; is that right?
A Yes. But I believe on the system it was actually called License.log.
Q What was this file?
A It looks like a Metasploit license keep or license log. You can see about eight lines down it says, license status

activation, okay. User warninggp@gmail.com. And it says, Metasploit community.

Q And Metasploit that was that suite of software you described like a Swiss Army knife a little while ago?

A Right. Metasploit is a very common hacking and pen testing tool.

Q I'm showing you what's in evidence as Government Exhibit 434. What is this document generally?

A So this is the output of a file -- so here it's basically listed as Mozilla_history.XLSX, but it's actually output from a file called Places.SQlight.

Q What is the significance of that?

A So it's basically just Mozilla history. This is the way that Mozilla, the web browser stores some of the activity that you participated in, sites you visited, things you've done. It's in something called the SQlight, which, surprise, is SQL-based. Basically it's a different flavor of SQL. It's just how Mozilla tends to store stuff locally.

And in this case what it is -- the output here is information it gathered, basically what we say is cached when somebody was using Mozilla. So you use your web browser your computer typically goes out to whatever site you want, gets the information it needs to display the images, right, CNN.com, all the photographs and the text, things like that, and usually the web browser does what's called caching and

stores some of that stuff locally.

You can clear the cache, but you don't have a whole lot of control about what the system does or doesn't cache. So basically when you visit a website, the browser will cache what it wants to cache and it wouldn't be something that would be obvious to you.

Q Did this particular entry from the cache reference that email address, warninggp@gmail.com?

A Right. So what you can see here is basically somebody went to mail dot-- sorry, I didn't mean to put an arrow there. You can see that somebody went to mail.Google.com, so Gmail, and there's some emails that came in, you know, learn how to use Metasploit community edition, warninggp@gmail.com. Another one says verify your email address.

THE COURT: Little slower, please.

A Sorry. It says: Learn how to use Metasploit community edition, which we saw in the earlier exhibit, and then it says in the email address warninggp@gmail.com, then another request to verify their email address and a number of other emails that appear to be associated with the email address warninggp@gmail.com.

Q There's an entry for, pretty Kiev girls at warninggp@gmail.com?

A Right. The structure of that is it's a little hard to tell because it looks like there might be some characters that

were in there they were in a different alphabet that this system doesn't display, that's why some of those look unusual. But, primarily, it looks like what you're looking at is a subject of an email and then the recipient.

So the subject was, you know, verify your email address, and the recipient was warninggp@gmail.com.

Q Just so it's clear, Agent Shahrani, these documents we're look at, these are instances on image 6B that show or suggest that the user used the email address warninggp@gmail.com?

A Right. What this basically suggests is somebody that had access to that email account logged into that account on this computer and in so doing using webmail and in so doing it left these artifacts behind.

Q Agent Shahrani, did you also conduct some forensic review of images of computers that were seized from the defendant, Vitaly Korchevsky's house on the day of his arrest on August 10, 2015?

A I did.

Q How did that process work generally?

A Pretty much the same. There were images that were taken of the systems and I reviewed them.

Q I apologize I think I misspoke, defendant Korchevsky arrested on August 11th, 2015; is that right?

A I believe so. I believe the images were taken during a search of the residence.

Q You weren't there for --
A No --
Q -- that particular search?
A -- no, I wasn't. That was conducted, I think, by our Computer Analysis Response Team, CART.
Q Did you subsequently review the images that were taken?
A I did.
Q What software did you use to conduct that review?
A FTK.
THE COURT: Sorry.
THE WITNESS: Oh, sorry, FTK, the Forensic Toolkit.
BY MR. TUCKER::
Q That's some of the same software that you told the jury about on Thursday?
A Right, the same style of software. I'm not sure if it was the exact same version, but...
Q May I just show the witness, Ms. Mulqueen, what's been marked for identification as Government's Exhibit 424.
THE COURTROOM DEPUTY: Witness only.
Q Do you recognize this document, Agent Shahrani?
A I do.
Q What is it?
A So there is basically -- there was basically, like we said with cache images, right, with cached data, this was a cached email.

Q And where was this image found?
A It was found -- I'm referring to my notes.
Q Which notes are you referring to?
A Sorry. So this is 3500SS-7.
Q Thank you.
A So this was found on -- this is 424, correct?
Q Correct.
A Yes. This was found on a image of a Dell computer.
Q Is this a fair and accurate copy of that fragment that was found on that Dell computer that you personally saw in your FTK review?
A Basically, just so you understand, the way that this stuff is found on the systems is -- so this was I believe a .HTM file and so it's basically a HTML code, right. So HTML is what most web pages are written in, so depending on the browser that you look at it in, it will look a little bit different, like what gets displayed might change a little bit, but in terms of this representing an accurate rendering of what you would get if you look at it now, yes. If you were looking at it through, you know, the webmail or something there might be more things -- you can see there are images that are missing with the question marks and things like that, but, yes, it's accurate.
MR. TUCKER: Your Honor, the government moves to admit Government's Exhibit 424.

THE COURT: 424. Any objection?

MR. HEALY: No objection, Your Honor.

THE COURT: Received.

(Government Exhibit 424, was received in evidence.)

MR. TUCKER: May we publish, Your Honor?

THE COURT: Yes.

(Exhibit published.)

BY MR. TUCKER::

Q So now that the jury can see, Agent Shahrani, you indicated the data missing, can you just explain so the jury can see what you mean by that?

A Yes. Like I said, this is an HTM -- it's a HTML file, right, so if you looked at just the raw data it would be very difficult to read as a human. So what this is is that this is basically what that HTML file looks like when you look at it through a web browser, but because this is excerpted from a webmail interface and the computer that we looked at it on wasn't connected to the Internet, there are certain things that are missing. Like in this particular case you can see it's displaying question marks where there would be some sort of image, a logo, something like that. But in terms of the substantive content, the text, it's accurate.

Q What's the email address I just highlighted on this document that was extracted from that Dell image file?

A Dubovoy1, that's D-U-B-O-V-O-Y, and then the number

1@gmail.com.

Q Looking at the second page, can you read this text from that same exhibit?

A Sure. It says Bill To: Igor Dubovoy, 6240 Crested Moss Drive, Alpharetta, Georgia, 30004, United States. Then there is a phone number (678)665-7771.

Q What is this document generally, Agent Shahrani, or what does it appear to be?

A It appears to be from receipt from Microsoft for buying Office365.

Q What's Office365?

A Office365 is a -- I guess you can go both ways. It's basically the latest version of Microsoft Office. I think it's web-based as well as something that you can download onto your home computer.

MR. TUCKER: Ms. Mulqueen, just for witness.

THE COURTROOM DEPUTY: Witness only.

Q I'm showing the witness what have been marked for identification as Government's Exhibit 418 --

A Okay.

Q -- and 426.

Do you recognize these documents, Agent Shahrani?

A I do.

Q Where did you find these?

A So these were taken from SC4, which was an image of a --

I'm sorry, I'm referring again to SS7. This is a Lenovo laptop that was imaged during that same search I referenced.

Q The Lenovo laptop that was imaged during the search of defendant Vitaly Korchevsky's residence?

A That's correct.

Q Are these fair and accurate copies of the data, certain data found on that image SC4?

A Yes. Again, with the same caveats since it's the webmail interface there are some things that aren't displayed properly but in terms of the text content, yes.

MR. TUCKER: Your Honor, the government moves to admit Government's Exhibit 418 and 426 and their corresponding translations 418T and 426T in evidence.

THE COURT: Any objection?

MR. BRILL: No objection.

THE COURT: They're received.

(Government Exhibit 418T and 426T, were received in evidence.)

MR. TUCKER: May I publish, Your Honor?

THE COURT: Go ahead.

(Exhibit published.)

BY MR. TUCKER::

Q Looking now at what's in evidence as Government Exhibit 418, this document is obviously not in English, but is there a reference to particular email address here?

A Right. You can see a reference to the email address VMARKEN, V-M-A-R-K-E-N@BK.ru.

Q Now looking at 418T, the English translation of that document, I'm going to turn your attention to really where it says, your computer has incorrect local time installed which is why your email interface is displayed incorrectly. We strongly recommend that you set the clock.

Did I read that right?

A That's correct.

Q Is there a reference here to that email address, VMARKEN@BK.RU?

A There is.

Q Now that the jury can see it, please explain what they're looking at here?

A Sure. As I said before, because of the way this is being displayed, the content is stored because it's an artifact, some things aren't being displayed properly here.

So when you're accessing webmail, something like Gmail or Yahoo email or something like that, there is a lot of stuff happening in the background that you don't see. There's kind of -- there's probably like a basic HTM, but a lot of the contents that you're seeing, the emails, your inbox, things like that, that's usually generated by some other kind of scripting language. Typically it's something like JavaScript.

So what you're seeing here is basically portions of

that JavaScript, portions of things that got downloaded with this file. And when we try to view it in our forensic software or whatever browser this was opened in, that script in the background looked around and realizing something was wrong and through up an error message. If you were looking at this properly, that is on the actual webmail system, you wouldn't see that.

Q Just so it's clear, Agent Shahrani, what is webmail?

A Right, so webmail is --

THE COURT: Give me a just a second. Ms. Brill, are you all right?

MS. BRILL: I'm trying to be. Thank you, Your Honor. Maybe one more sip of water.

THE COURT: Maybe one more sip, maybe not.

If you need a break just wave. We're going to take a break in 10 minutes unless you need one now.

MS. BRILL: I think it worked. Thank you, Your Honor.

THE COURT: Okay. I'm sorry. Go ahead.

BY MR. TUCKER::

Q What's webmail, Agent Shahrani?

A Webmail is basically a web-based email system. Most people today probably are more familiar with webmail than the traditional versions of email, but in a very short summary of it: You have a couple of different systems you can use when

you read your email, right. Old style when you were connecting to IMAP, like Internet mail application service, your computer would reach out to the mail server, download a copy of all the emails and store it locally. Your phones, other devices things like that probably still do that. They reach out and get a copy of either the protocol called POP and there's a protocol called IMAP. But in general, basically they reach out, they get a copy of the mail and they store it locally.

With the rise of webmail, that's different. So you can -- if you've accessed your, say, Gmail or Yahoo mail, or whatever, or hotmail account from a web browser, those messages aren't really being downloaded to your computer, they are being shown, they're being displayed to you, like you can see them, but there aren't like duplicate copies of that stored locally and pretty much when you close the web browser your system loses access to those mails.

Now, obviously, there are other things that you can set and configure so that you can have that mail copied to you locally, but fundamentally if you're using a webmail interface, you see the emails, they are stored on the remote server, they stay there, you look at them, when you're done the web browser closes and the only thing that will be left on the local computer would be, as I said, artifacts, things were that cached, bits and pieces that are left behind by the

browser.

Q Like what we're looking at here in Government Exhibit 418?

A Correct.

Q And showing you what's in evidence as 426 and 426T. Is that the same sort of thing, Agent Shahrani?

A Right, so same sort of thing. This came from -- this is a file that was listed as, basically in short, inbox then to a square parenthesis around a one. So inbox square parenthesis, number one, close parentheses, dot HTM. So same kind of thing, right.

This is -- you can see across the top here in the translated version, this look likes it's kind of the navigation bar at the top of an email system like you'd expect, or if not the navigation bar the interface, and then it also has at the end of it the username or the email address VMARKEN@BK.RU.

Q Agent Shahrani, what's metadata?

A Metadata is data about data. So if -- lets take an example that's been in the news somewhat, right. So if you talk about a phone call, the phone call itself, the conversation that a person has with another person, that would be the data, right, that's the content of the call. But the metadata for that would be the time that the call was placed, the duration of the call, where the two people were, right, if

it's a cellular conversation, the GPS location or other location data for one party and that same data for the other party. So basically it's information about the file itself or about something. It doesn't necessarily have to be a file, you could have metadata about lots of different things.

Q Were you able to identify any metadata associated with Government's Exhibit 418?

A Yes.

Q And did that metadata include a last modified date?

A Yes.

Q What did you learn?

A The last modified date was mid 2012 or -- yeah.

Q The last modified date for this document?

A I believe so was -- sorry, I'd have to refer.

Q Okay.

MR. TUCKER: May I just have moment, Your Honor?

THE COURT: Yes.

Q Agent Shahrani, one other question here, this domain VK.RU, what's the significance of that?

A It's a Russian email provider, I believe.

MR. TUCKER: Your Honor, if I could have just one moment. I apologize trying to find something or I'll just move on. Seems not.

Q Agent Shahrani, just so we're clear, Government Exhibit 418, sitting here today, do you remember the date

modified for this particular document?
A I don't.
Q Agent Shahrani, we talked about a few specific examples of files that you were able to find on images associated with the defendant Korchevsky's media; is that right?
A That's correct.
Q Is that everything that you looked at on Korchevsky's media?
A No.
Q Was that everything that the FBI was able to identify --
A Yes.
Q -- on Korchevsky's media?
MR. TUCKER: Just one moment, Your Honor.
Could I just show the witness, Ms. Mulqueen?
THE COURTROOM DEPUTY: Witness only.
MR. TUCKER: Witness only.
Q I'm showing the witness what's been marked for identification as Government's Exhibit 4 -- 826.
THE COURTROOM DEPUTY: 8-2-6.
MR. TUCKER: 8-2-6.
Q Agent Shahrani, turning to the second page of this document, do you recognize that entry?
A I do.
Q Now, agent Shahrani, what is Government's Exhibit 826?
A This looks like it could be metadata for the file I

mentioned, inbox with the parenthesis number 2.HTM.

Q So it's clear, that was Government Exhibit 418; is that right?

MR. HEALY: Objection.

THE COURT: What's the objection?

MR. HEALY: I don't believe that's what the witness said. I believe that's --

THE COURT: I understand him to be referring -- tell us exactly -- first of all, lets go back to 826 --

MR. TUCKER: Yes.

THE COURT: -- what is it?

BY MR. TUCKER::

Q What is Government's Exhibit 826?

A That's the metadata for the exhibit that you showed just before this.

Q So that's -- you were testifying earlier about data?

A Right, if you set it down again --

THE COURT: The metadata for 418 in evidence?

THE WITNESS: Correct. So this is the metadata, as I said, that 418 was originally stored as inbox with the parentheses 2.HTM. This is the metadata for that.

THE COURT: Clear, Mr. Healy.

MR. HEALY: Yes, Your Honor.

MR. TUCKER: Your Honor, the government offers Government's Exhibit 826.

THE COURT: Any objection?

MR. HEALY: No objection, Your Honor.

THE COURT: Received 826 in evidence.

(Government Exhibit 826, was received in evidence.)

MR. TUCKER: May we publish, Your Honor?

THE COURT: Go ahead.

(Exhibit published.)

THE COURT: Go ahead, then we will take your break.

MR. TUCKER: This is my last question, Your Honor -- my last two.

So, Agent Shahrani, this makes reference to that domain that you mentioned earlier, inbox bracket 2.HTM; is that right?

A That's correct.

Q Does this reflect the metadata you were testifying about earlier of last modified?

A Yes. That's December 10th, 2014 at 16:25 eastern standard time.

Q So it's clear, that's the last modified time of this Government's Exhibit 418 which is in evidence?

A Correct.

Q And, Agent Shahrani, would you explain to the jury the limitations of the last modified and what it means?

A Sure. So last modified depends on a lot of variables, right. Depending on how the system is configured, whether the

date and time on the local computer are set properly. So if everything is set correctly on the system, then typically the last modified date reflects accurately, but what a modification is depends on what some of the systems are, right? So if the file is copied, there are other stages or other steps that can be done to a file that could change it. But, typically, the last modified date is the last time the file was modified. So if it's sitting there and nothing has been done to it, it hasn't been edited or changed typically the last modified date reflects that.

MR. TUCKER: No further questions, Your Honor.

THE COURT: All right. We will take our mid-morning break, folks, do not discuss the case. We will resume in about 12 minutes.

THE COURTROOM DEPUTY: All rise.

(Jury exits courtroom.)

THE COURT: Okay, you can step down for a few minutes.

THE WITNESS: Thank you, Your Honor.

THE COURT: I think, folks, relative to the gentleman I discussed earlier in the morning, I think maybe the best way to do this would be to take a few minute -- to break for lunch just a few minutes early, I think it would be less apparent to the rest of the jurors. Do you all have a view on whether or not you want to do this in open court or

defer to the courtroom and the court reporter.

MR. BRILL: For Mr. Korchevsky, we have no problem with the Court in private speaking to the juror initially.

THE COURT: Yes, of course. And you'll get that conversation of course.

Ms. Whalen, you're views.

MS. WHALEN: Our preference would be to do it in open court, Your Honor.

THE COURT: Then we will do it in open court.

MS. WHALEN: Thank you.

(Recess.)

(Continued on the next page.)

(The following takes place out of the presence of the jury.)

THE COURT: Where is our witness?

MR. TUCKER: He's out in the hall, Judge.

THE COURT: Have a seat, folks, while we await the witness.

(Pause in the proceedings.)

THE COURT: Here he comes.

(Witness enters courtroom.)

THE COURT: I tell you I keep the whip cracking, right. I guess I have to tell everybody else too.

(Witness resumes the stand.)

THE COURT: All right, cross-examine.

MR. HEALY: Thank you, Your Honor.

(Pause while counsel confer.)

CROSS-EXAMINATION

BY MR. HEALY:

Q Good afternoon, Agent Shahrani.

A Good afternoon, counselor.

Q I'd like to start with something that I think that I'm on firm footing here, I want to talk about IP addresses and hot spots.

A Okay.

Q You told the government on direct that an IP hot spot allows someone to have a different IP address than their home

IP address; is that correct?
A Typically, yes.
Q But you agree with me that people buy mobile hot spots for reasons other than concealing their home Wi-Fi IP address, correct?
A Yes.
Q In fact, people buy mobile hot spots so that they can have access to the internet when they may not have Wi-Fi service; is that correct?
A Yes.
Q Perhaps when they're traveling?
A Yes.
Q And you'd also agree with me that any time you log in from a mobile device or a computer when you're not at home, you're going to get a different IP address than your home IP address?
A Assuming that you don't VPN into your home computer and then connect through that, yes.
Q Absolutely assuming that.

You'd agree with me that, for example, anybody that's logged in through the Eastern District of New York Wi-Fi will have a different IP address than their home IP address.
A Yes.
Q In fact, they'll have the same IP address, correct?

THE COURT: Same IP address?

A Excuse me?

Q The same IP address.

If you've logged into this Wi-Fi, this Eastern District of New York Wi-Fi, anyone who logs into that will have the same IP address, correct?

A Depending on how the server is configured, so there are a lot of variables to what you're asking.

Q I'll withdraw that. We don't need any more details.

A Yeah.

Q I want to start with talking about the two computers that you examined that were seized on August 11th, 2015. I believe you told us that you examined a Lenovo computer?

A Yes, SC-5 and SC-40.

Q Yes.

A Yes.

Q And you examined a Dell computer?

A That's correct.

Q And when you examined those, you found some artifacts that referred to a VMarken?

A That's correct.

Q I want to talk about those in a moment. I'd like to talk about specifically some other things.

Would you agree with me that the hard copy images from those computers occupy tens of thousands of pages?

A Assuming that you could put some of that content and print it out, sure.

Q And when you searched those tens of thousands of pages, you were searching for connections that would tie those computers to the hackers; is that correct?

A We would search for a variety of different things. We would be looking for information, yes, that might tie them to the hackers but other information that's also relevant to the investigation. It is not an either/or kind of possibility. You'd look for anything that might be relevant to the investigation.

Q I didn't mean to imply exclusively, I just wanted to know if you searched for evidence tying the computers to the hackers and I think you told us yes.

Did you find any evidence of Loscal?

A No.

Q And you didn't find any evidence of Rupion?

A No.

Q You didn't find any evidence of the IP address 83.133.126.96?

A That's a remarkably specific question that without reference I couldn't say one way or the other.

Q Were you even asked to look for that?

A Without referring to notes, I don't know.

Q You didn't find any evidence of Warning GP, did you?

A On the SC-4 and SC-5 systems?
Q Correct.
A No.
Q You didn't find any evidence of Vladimir Kopienko (ph)?
A No.
Q You didn't find any evidence of an email address vip2000?
A No.
Q You didn't find any evidence of an email address stargate11?
A No.
Q You didn't find any evidence of an email address positive1?
A No.
Q You didn't find any evidence of Valera Pychnenko?
A No.
Q You didn't find any evidence of Vaiobro?
A No. But that being said, the Vaiobro name wouldn't necessarily -- that's s chat name, not a computer name or system name.
Q But you didn't find it?
A Correct.
Q Now, you testified you're aware those two computers, the Lenovo and the Dell, were seized on August 11, 2015, correct?
A I don't recall the exact date but they were seized pursuant to a search at the defendant's residence.

Q And --
A Or, excuse me, the computers themselves were imaged, I don't believe the computers themselves were seized. I believe they were copied and then I reviewed those copied images.
Q Would you agree with me if they were seized subject to a search warrant, they were no longer in the possession of the person who had them prior to the seizure?
A Well, as I said, I don't believe that the systems were physically seized, I believe that they were imaged and normally if a system is imaged in place the system remains with the user or the owner.
Q Fair enough.

From your examination of those two computers, you don't know who had them prior -- who had possession of them prior to August 11th, 2015, do you?
A When you say those two computers, do you mean SC-4 and SC-5 or do you mean the original, the War and Alex PC systems?
Q No, no, we're still talking about the Dell and Lenovo, I'd like to just use those.
A Sure, I just want to make sure we're talking about the same thing. Could you repeat the question.
Q From your examination of those two computers, you have no information, no evidence as to who actually possessed them prior to their being seized and imaged on August 11, 2015?
A There was data on there from -- well, I mean there was

personal data relating to individuals on the system but I'm not sure exactly what you mean by proof of who owned the systems before then -- that date.

Q I wasn't asking for proof, I was just asking if you had any information that on a given day, let's say April 3rd, 2012, who actually was in possession of that computer?

A Not that I'm aware of, no.

Q And you don't actually know who purchased that computer based on your examination of the images?

A No, based on the examination of the images I don't but that doesn't mean we don't have that information from another method.

Q But you yourself?

A No, I personally have no idea.

Q And you yourself don't know who installed anything on either of those computers?

A No, I don't.

Q Now, you told us that on the Dell computer you extracted something that's in evidence as --

MR. HEALY: This is in evidence, Ms. Mulqueen.

THE CLERK: Certainly.

Q It's in evidence as 424.

A Correct.

Q And we refer to this -- you referred to this as Office 365?

A A receipt for the purchase.
Q A receipt for Office 365. Now, you don't know who installed this on that Dell computer, do you?
A No.
Q And you don't know who was in possession of the computer when it was installed, do you?
A No, I don't.
Q You do know or we do know from this exhibit that it was billed to Igor Dubovoy, correct?
A That's the email address listed, yes.
Q Now, you also talked about a couple of artifacts that were found on the Lenovo computer, do you recall that?
A I do.
Q And I'm going to show you what is in evidence as Exhibit 418 and this is the original version which is in Cyrillic.

MR. HEALY: Mr. Tucker, could I get the translated version which would be 418-T?

(Pause.)

MR. HEALY: This is 418-T.

Q I just want to make sure that we are referring to the same exhibit. Is this the exhibit that corresponds to the metadata that you told the jury about in 836, this particular original artifact?
A No, I believe the metadata was for 426 -- no, I'm sorry,

yeah, it's 418.

Q It was this exhibit?

A Yeah, I believe so.

Q This one says that says Registration Log in here, this one?

A Yeah, that's what you're saying is 418?

Q Yes.

A I believe so, yes.

Q And I believe you told the jury that the message that Mr. Tucker highlighted and it's still highlighted that "your computer has the incorrect local time installed" popped up because the system ascertained that the incorrect local time was installed?

A Well, no. So, what it is is -- how to explain this -- so, if you looked at this file as the raw html, right, the raw code, you wouldn't see that message because that code, there's a little piece of java script or some kind of code that is running, when you open this up in a web browser it runs, and because we were looking at it in a forensic box -- a forensic review system, that script in the background noticed that something was off, basically it couldn't communicate with its home server because our forensics systems are not connected to the internet so it can't ping out and get like the date and time information, all the stuff it is wanting, so it just generated an error message. If you looked at the raw html

code, you'd see that error message and a variety of other potential error messages in there because the raw code contains most of what could be displayed. So, that doesn't mean that the individual computer that this file was recovered from had a time and date setting correctly, it means that because we tried to display it on our forensic computer in a human readable format as opposed to giving it as a very jumbled html file, the browser read some of the code and generated that error message because it couldn't talk out to what it expected to. That doesn't mean that the system itself it was recovered from had a misconfigured time key.

Q So, basically that has no significance, that statement at the top of that?

A Correct.

Q So, it could have had a correct date and time code or it could have had an incorrect date and time code?

A Yeah, basically, like I said, it is an artifact, that's all it is. If you looked at this on a normal system or on the system itself, you probably wouldn't have seen it or you might have seen it on the system itself because it wasn't able to talk out to the servers it was expecting to. Like I said, with web mail there's a lot of stuff that's loaded behind scenes so when you get an artifact, depending on how you display it, there's lots of things that you would never normally see unless there was an error.

Q But you did tell us that 836, which had a date and time in December of 2014, that actually may be an incorrect date and time?

A The metadata for the file, that's what was displayed but without knowing more details about the nature of the system and some of the configurations, I can't say that that was certainly the time.

Q That's all I wanted to know, we don't know for certain that that's the correct date and time.

A Right, without more information, no.

Q I want to turn for a minute and talk a little bit about 4-A and 6-B, those are the computers that I might refer to as the Alex PC and the War PC.

A Okay.

Q Now, and if you need, by the way, Agent, to refer to the SS-2 and SS-3, that's fine, I know you were referring to those on your direct testimony.

A Okay.

Q I want to talk first about the Alex PC which is 4-A.

A Okay.

Q So, in your examination of the Alex PC or in your verification of the original examination of the Alex PC, would you agree with me that the computer is only indicated potentially for being used as intrusion between November of '11 and November of 2012. And if you want, you can refer

to page one, I believe that's contained in the report on page one.

A So, yeah, no, I think that's fair.

Q But, in fact, as you testified, the three newswire services that we've been talking about, PR Newswire, Business Wire and Marketwired, actually have indications that are significantly after the first indication, significantly after November of 2011, correct?

A I don't know of the exact dates for some of those intrusions.

Q Well, if we look at what you testified to, I believe you told the jury -- and I believe this is indicated on page nine of SS-2 -- that the first indication of an SQL report -- and if I use the wrong language, please correct me -- the first indication of an SQL report was actually in March of 2012; is that correct?

A Right, yeah, there's a file here, r2b2hn.com.

Q Then the first indication of a PR Newswire SQL report was in May, May 30th of 2012? I believe that's on page 19.

A That appears -- sorry, what was the date again?

Q I believe you said it was May 30th, 2012; is that correct?

A Yes, that appears to be.

Q And although the report indicates that the last date that that computer, that Alex PC had access or made an intrusion

attempt was in November of 2012, in fact the report limits even further when it was used in conjunction with each newswire service; so, for example, Business Wire, the last intrusion evidence is September 8th of 2012, and again would be page nine?

A In, let's see, some of the chat history -- if you're saying September 8 of 2012, I think that's just referencing chat history --

Q Well, it could be earlier; can you tell from that when the last SQL intrusion was?

A The last record on here says -- or the last that's noted on this particular one seems to be March 24th of 2012, that's the last SQL map. I should note that just because an SQL map was run on that date, that doesn't mean that the information gathered from the SQL map was not used at a later date and time to commit an intrusion. These are the logs -- like you wouldn't need to rerun the SQL map multiple times over a period of time to get this, you could run it once or twice, get the information you needed and then use that information at a letter date and there wouldn't necessarily be log files or any records left on the system of that event.

Q Depending on what the information was?

A Right, depending on what the information was and depending on what tools you used.

Q So, in fact we'll talk about that in a bit.

I also think that that report that you reviewed and verified indicates that the hackers reached different levels of access on the different servers, is that fair to say?

A In the conversation they had they discussed certain levels of penetration that they mentioned in the system and also discussed elevating their privileges which is a fairly common tactic.

Q When you say "they" discussed, who is "they"?

A The conversations that are occurring between the hackers or the individuals.

Q Fair enough. I'm actually talking about what the forensic examination determined which you said you reviewed is that, as I understand it, that, for example, the finding was that PR Newswire was researched, is that fair to say?

A You could use the term researched, you could say scanned, you could say cased, that would be synonymous.

Q That's a fairly low level of access, correct?

A It would -- I would say it is more of a preliminary step as opposed to -- like I said, it is similar to casing a location, you're not maybe breaking into it but you're looking for vulnerabilities, you're looking for weaknesses, so it would be an early step in the intrusion process.

Q And that Marketwired and Business Wire had been accessed is the term that I believe was used in the report?

A That's correct.

Q But none of those domains were actually compromised which is the highest level, correct, according to that report? There's a table on page eight if it refreshes your recollection.

A Right. So, according to the information -- well, again, there's kind of a semantics issue here where if you say you accessed the system without further details is something that can have many different meanings; you can be a hacker and say that you successfully accessed the system by breaking into it, you could also say you accessed the system by logging on to their public website. In the context of hackers, typically if you're saying you accessed a system, it means you breached it, but without more context I couldn't say.

Q You couldn't say whether any of those reached the level of compromise, that was my question?

A Sorry. So, yes, if you're asking if these were SQL -- the SQL map sessions were compromised, there were database dumps that were present on there which would indicate that the systems -- that that data had been extracted from the target systems which would indicate that there was some kind of compromise.

Q So, are you saying that that report is incorrect?

A No, I'm saying it is a semantic differential, saying a system was accessed can have many meanings, it is not a -- it is an open term that could be interpreted several different

ways.

Q We'll disregard the table in the chart then.

Let's talk about it this way. You talked about data dumps and documents; those documents aren't necessarily press releases, correct?

A No, those documents -- so, some of the documents we discussed were user names, passwords, login-s, things that you would need to access the system to obtain press releases and other content.

Q Or try to access the system?

A Or attempt to access the system. Although having those user names and passwords in and of themselves would suggest that there had been an access of information that the ultimate user, that the typical user wouldn't have access to, that they would have had to have done something to obtain that information.

Q Absolutely, Agent, I don't mean to imply that there was no hacking going on. I'm just trying to get a little more precision on exactly when and where things were done.

And before we move on to the War computer, can we agree that any data that was taken off of the newswire services from this particular computer had to happen in the case of Business Wire after March of 2012?

A Based off of the records that we were able to locate, the materials that we were able to see on the system, that's

consistent but that doesn't mean there weren't other systems used that the hackers didn't -- basically that's off of what we have here.

Q That's my question, off of this computer?

A Off of this information, that's correct.

Q And for PR Newswire, for this particular computer, any information that was obtained had to be after May 30th of 2012, that was the date you told us?

A Well, on or after.

Q I'm happy to go with on or after.

A Sure.

Q And with Marketwired, where I don't believe you told us and we'll just go with general first evidence of intrusion, May 15th of 2012?

A That sounds correct, yes.

Q Let's talk briefly about the War computer, that would be of 6-B. You want to refer to SS-3 is the report you're referring to.

A Okay.

Q So, according to the indications in the forensic review of that computer, the first instance of any malicious activity was in February 20th -- on or about February 20th, 2012; is that correct?

A Yes, I believe -- let me verify that, yes. You said February --

Q 20th. On page one.

(Pause.)

A Yeah, I'm looking at the actual original, the session info. Yes, that sounds correct.

Q And you told the jury that actually with respect to each newswire service, the dates are somewhat later. So, for Marketwired you told us the first SQL intrusion was on May 2nd of 2012; is that correct?

A I believe so.

Q And that for Business Wire it was in March of 2012?

A That sounds correct.

Q And for PR Newswire it was in March also of 2012, March 26th?

A Yes, let me double-check just to make sure.

Q That would be on page 37 if I'm not mistaken.

A Yes, sounds right.

Q And then the last intrusion for anything on this computer that there's any forensic evidence is October 19th of 2012?

A That sounds correct but, again, I'd like to clarify. The last -- saying that the last intrusion is just the last scan, the last logs, the records on here, that doesn't mean there weren't other intrusions. I'm just saying from the records here.

Q From the records you reviewed, that's all we can ask you to talk about.

A Yeah.
Q So, to be clear finally, any information that was obtained by this War computer, 6-B, for Marketwired had to have been obtained after May 2nd of 2012?
A On this particular computer?
Q Yes?
A Yes.
Q Only referring to this particular computer.
A Yes.
Q And then on Business Wire I believe it is March 19th of 2012?
A That's correct.
Q And PR Newswire on March 26 of 2012?
A That's correct.

MR. HEALY: No further questions.

THE COURT: All right.

Ms. Whalen.

(Continued on next page.)

CROSS-EXAMINATION

BY MS. WHALEN:

Q Good afternoon.

A Good afternoon, counsel.

Q I'm going to show you what's been previously marked and entered into evidence as Government Exhibit 323.

A Okay.

Q And I think you were asked about it on Thursday of last week.

A That's correct.

Q Okay. And so at the top of the document, you testified that this was sent from the e-mail address of Vladislav Khalupsky?

A According to the header information, yes.

Q And then it was sent on December 12th -- December 18th, 2013?

A Correct.

Q And --

A Again, based on the header.

Q Based on the header.

So let's -- assuming -- we are just reading into evidence what the header says.

A Yes.

Q And that it was at 1:52 p.m., correct?

A Right, but with an unknown time zone.

Q That's correct. I believe that was your testimony on Thursday.
A That's correct.
Q And it was sent to the address vkhalupsky2002@yahoo.com, according to the header.
A Correct.
Q And just going to the second page, I think you also reviewed this in your testimony on Thursday, correct?
A Yes.
Q Okay. And you saw, and I believe you were asked about, dolphintenet.odessa.ua, correct?
A Yes, I was.
Q And there's a series of numbers, 195.138.72.114, correct?
A Correct. That's an IP address.
Q That's an IP address, great.

There's also what appears to be an IP address in front of it. It's 192.168.0.100, correct?

A That's correct.
Q Now, first going back to dolphintenetodessa.UA. TENET.UA is a telecommunications company in Ukraine, correct?
A If you say so. I'm sorry, I'm not intimately familiar with --

THE COURT: If you don't know, I don't know.

A Okay. I don't know.
Q Did you do any investigation into -- I'm assuming you did

not do any investigation since you don't know about it.
A Correct.
Q And this -- trying to get information about this company was not part of the mutual legal assistance treaty activity that you -- that took place in this case, correct?
A I don't know.
Q Looking at this IP address, since you didn't do any investigation into TENET, you don't know how many individuals or how many devices could be connected to this IP address, correct?
A I have no idea.
Q And then this other IP address 192.168.0.100, that's part of a series of IP addresses that are reserved for private Internets, correct?
A Yeah. Typically -- it's called reserve address, so that basically suggests that it's an internal network. In this case, since this is Webmail and it's Google, it might be a Google internal IP address. Basically, there were public facing IP addresses that everybody is kind of familiar with, and then there's a reserved or series of reserved internal blocks that you are supposed to use inside of your network, and that would be one of those reserved addresses.
Q Okay. And so -- while this address 19513872114 would be unique --
A Typically, that's a public facing IP address, so that

would be unique on the Internet -- unique on the public Internet. That doesn't mean that somebody couldn't set up their own you know weird internal network and then reassign that. But, yes, in terms of something you could access on the Internet, that would be unique.

Q And so generally, though, these 192.168 numbers, they can be repeated in internal networks from business to business, correct?

A Sure. If we all went to our individual homes and if you had, like, a Wi-Fi router and you had multiple devices connected to that, all of us would probably have a 192 address, something internal to that network. That's fairly standard.

Q Now, there was also some discussion about time of this -- the time of this e-mail, and I think, as you indicated, on the header on the front of the e-mail, it says 1:52 p.m., correct?

A Correct.

Q But we have no direct information because we don't know what time zone, correct?

A Right. But I think if you look at the header, it will give you the time zone.

Q Okay. And so just going through the time zone, we have a time at the top, the first line, 10:52.28 2013.

A Mm-hmm.

Q We then have another time above the line that says

content-type. Again, it says, Wednesday, December 18, 2013, and that gives 10:52.27, correct?

A Yeah.

Q And that has a minus 0800, and you indicated that that was Pacific Standard Time, correct?

A Yeah. Minus 800 is -- most servers are run on, as I said, UTC, Universal Time Code, it's basically Greenwich Mean Time, and that way you can -- no matter where your server is, everybody is kind of operating off of the same time code. You basically have to have something like that set up otherwise the Internet doesn't really work. So, in this case, the time would be 10:52.27 or 10:52.28 depending on when it moved from server to server. There's -- obviously, if somebody moves from one server to another, there's a little bit of lag time.

Q And then there's one more time down four -- four lines from the bottom next to -- it says date, and it says, Wednesday, 18, December 2013, 20 52 27 and then it has plus 0200, correct?

A That's correct.

Q And that would be UTC plus two hours, correct?

A Correct. I'm not sure exactly what the non-UTC time zone would be. It's somewhere in Europe, I would assume.

Q You have no knowledge -- you have no personal knowledge that this is the time zone in Ukraine, correct?

A Yeah. I'm sorry, I don't know what the time zone is

Ukraine is.

Q And then I'm also going to show you -- it's been marked -- what's been admitted into evidence as Government Exhibit 323-A1, and you've seen this before, correct?

A Yes, I have, on Thursday.

Q And this was -- I believe this was the attachment to 323?

A Yes.

Q And I believe that you testified -- and I believe you testified that there were letters "E N" displayed on the monitor.

A Yes. You can see them there.

Q And I believe that it was your testimony that this meant that the computer was configured to English, correct?

A Well, if you have that in the lower corner, that's basically a setting that you can change, so you can toggle what language it displays. Normally, for most of us, if you are a monolingual user, you don't have the language packs installed, so that doesn't appear. If you are bilingual or speak multiple languages or are working in multiple languages for whatever reason, you can install a language pack, and then normally the option to switch between the languages can be presented.

Q Okay.

So this is a setting that can be changed on the computer, the language of display, correct?

A Yeah. That's -- I think it's a setting in the control panel for Windows. You can configure it to display in whatever language you have a pack installed for.

Q Okay.

And then also --

A And you also might have to install those language packs to have foreign languages displayed properly in general. For instance, Cyrillic Arabic, sometimes you have to install a pack otherwise the data looks kind of garbled.

Q And let's just -- sorry. I think you testified as to the time in the corner being 1:25 p.m., correct?

A That's what's it's displaying, yes.

Q I think as you're saying, we don't know that that's the actual time. That's just the time that the computer is configured to, correct?

A That's correct.

Q Okay. And then also, I believe, you testified today -- oh, here it is -- you testified as to on the left-hand side of the exhibit, sort of the last icon displayed on the left-hand side, I think you testified that that was a WinZip icon?

A I'm sorry, you mean the right-hand side?

Q I'm sorry, I have real problems with right and left.

A Okay.

Q So --

A Yes. So on the right, as we're looking at the exhibit,

the rightmost icon?

Q Yes.

A Okay.

Q Is that the WinZip?

A It appears to be.

Q And that's -- I think you testified that that was a way to look at files that had been compressed through the zip program, correct?

A Yeah. WinZip can both compress and decompress files.

Q And then -- and I believe also you testified that -- I think it was on Thursday -- as to the date of the computer.

A Right. It looks like it's displayed as 18 12 2013, so it's a European kind of date format.

Q And then today, you testified about a number of -- you testified somewhat on Thursday and then again today about a number of computers that had been imaged that you had reviewed, correct?

A That's correct.

Q And you testified, I believe, about 4-A?

A Yes. 4-A was Alex PC.

Q Alex PC.

And then you testified about 6-B which, I think, was named War?

A Yes.

Q And these two -- these two images were from laptops that

were seized in Kiev, Ukraine, correct?
A I don't know if they were laptops. I just know they were personal computers.
Q But some kind of personal computer that was seized pursuant to a mutual legal assistance treaty search, correct?
A I believe so, yes.
Q And they were seized in Ukraine, correct?
A I believe so, but that's a -- that's what I was told, but you would have to speak with the --
Q So you have no personal knowledge as to where it is.
A Correct.
Q But in reviewing the images of these computers, you were able to determine the last date that the computers had been accessed, correct?
A That's correct, yeah, we discussed that.
Q And I believe that 4-A was last accessed on November 16th, 2012?
A Yes, that's correct.
Q Okay. And 6B was last accessed on December 19th, 2012?
A October 19th, 2012.
Q October, sorry.
And then you were asked to review a number of exhibits -- I'm just going to list them. You were asked to review them today. 437, 408, and 409.
A Yes.

Q Government Exhibit 411 and 444?
A Yes. The output files from SQLmap.
Q So those were the output files from the computers, or at least one of the computers, that was seized, you believe, in Ukraine, correct?
A Yes.
Q And then you also looked at 413, 407 and 407-T?
A Yes.
Q 427, 405, and 406-T?
A Yes.
Q And then 431, 432, 433, 434, and 435, correct?
A Correct.
Q And all of those were files from the Alex PC or the War PC, correct?
A Correct.
Q And all of those files were in the computers that were seized on November 16th, 2012, correct?
A Yes. They were -- the files that were provided to me that were seized and provided to the secret service and then to us.
Q So in any event, the folders that you saw, all of those government exhibits that I just referred to, all of those exhibits came from the computers that you reviewed and the images of those computers?
A Yes, that's correct.

Q Alex PC and War, correct?
A Correct.
Q Those files were contained in the computers that were last accessed on November 16th, 2012, and October 19th, 2012.
A Correct.
MS. WHALEN: No further questions.
THE COURT: I'm sorry, did you say you are finished? Ms. Whalen?
MS. WHALEN: I'm sorry. I said no further questions. I apologize.
THE COURT: Thank you.
All right. Any redirect?
MR. TUCKER: No, Your Honor.
THE COURT: Thank you, sir. You may step down.
Next witness.
(Witness steps down.)
THE COURT: Who is the next witness?
MS. NESTOR: Your Honor, the government calls Louis DiPietro.
(Short pause.)
THE COURTROOM DEPUTY: Good afternoon, sir. I'm going to ask you to please step my way. I'm going to ask you to please take the stand and raise your right hand.
(Witness takes the stand.)
(Witness takes the witness stand.)

LOUIS DIPIETRO, called as a witness, having been first duly sworn/affirmed, was examined and testified as follows:

follows:

THE WITNESS: I do.

THE COURTROOM DEPUTY: Thank you. Please have a seat.

State and spell your name for the record.

THE WITNESS: Sure. It's Louis DiPietro, L-O-U-I-S, DiPietro, D-I-P-I-E-T-R-O.

THE COURT: Go ahead, Ms. Nestor.

MS. NESTOR: Thank you, Your Honor.

DIRECT EXAMINATION

BY MS. NESTOR:

Q Good afternoon, Mr. DiPietro.

A Good afternoon.

Q Where do you work?

A I work for Panera Bread Company.

Q What is Panera?

A Panera is a bakery/caf restaurant concept that owns, operates, and franchises bakery cafs.

Q Where are you based out of?

A Needham, Massachusetts.

Q And where are Panera's headquarters?

A In St. Louis, Missouri.

Q What do you actually do for Panera?

A I am the general counsel.
Q How long have you been with Panera?
A Twelve years roughly.
Q I'm sorry?
A Just over 12 years.
Q How long have you been general counsel at Panera?
A About last three and a half years.
Q So what is your role being general counsel of Panera?
A I manage the legal department at Panera, supervise attorneys, and am responsible for all legal matters related to Panera Bread Company.
Q And prior to being general counsel, what was your role at Panera?
A I was the deputy general counsel and I had similar duties.
Q Between January 2010 and July 2017, was Panera a public company?
A Yes.
Q As part of your responsibilities as general counsel, back before 2017, were you familiar with the earnings process for Panera?
A Yes.
Q Please explain what your role was.
A I participated in the drafting and reviewing and approval of quarterly earnings releases through that entire process.

Q Did you also participate in the drafting and approval of other press releases?
A I -- other nonfinancial press releases, I would approve them. I wasn't as actively involved in the drafting of those press releases.
Q How did the earnings process at Panera work generally?
A Once the financial quarter ended, the financial results would be finalized, and then between that time and the ultimate earnings release, we would begin the process of finalizing the information to be included in the press release, press releases would then be drafted, they would be drafted, rewritten, then would go through a number of different levels of approval through internal and external advisors. Once the press release was then completed, it would then be sent to -- for distribution.
Q And how -- would there be a significant steps in the approval process once it was finalized?
A Yes. It would have to be approved by the finance department; the chief financial officer; myself, the general counsel; as well as external auditors and external legal counsel.
Q Generally speaking, what information is included in the earnings press releases?
A Earnings press release would -- first and foremost, it would include the main information, included would be the

financial results, so the revenues, profits, loss -- or loss, as well as other important key financial metrics which my be important in the industry, so comparable store sales or margins or other related financial metrics.

Q And what's a point of releasing earnings?

A It is the way that we distribute financial results to the investment community. We -- that is the manner in which, through that and through SEC filings, we announce to the public how we performed in a given quarter.

Q Is it relevant to your shareholders?

A Yes.

Q And explain that, please.

A So we would announce our -- the date that we would be releasing earnings so that that was on the calendar clearly of our analysts and/or the investor community. We would then release our earnings and they would anticipate those, they would -- we would issue guidance previously of what we expected throughout the year so investors were interested in seeing whether or not we delivered according to what we told investors we expected would occur, so it was a very important, and it was followed by a conference call with investors and analysts the day after we would release those earnings to ask questions about them.

Q Was the integrity of earnings releases important to Panera?

A Yes.
Q Why?
A It was important because it was -- because our financial results were first and foremost important to shareholders.

Additionally, it was important for the integrity of our earnings and our financial results that we had an opportunity to disclose and to discuss with franchise -- I'm sorry -- with shareholders, how our results were, how we were performing and how we were -- whether or not we were meeting the expectations of investors and if our business was performing well generally.

Q Were the earnings releases kept confidential within Panera?
A Yes.
Q Tell us about how that requirement existed within Panera generally.
A Well, we had a broader policy of confidentiality, particularly around earnings releases and financial results, given the materiality of the information. So individuals who work for the company were required to keep the information confidential and to also not use that information as well. They could not use the information regarding earnings to trade or otherwise participate, sell, or buy stock, or disclose that information, period, whether or not for the intent of making a sale or a purchase, but keeping that confidential for the

purposes I just discussed about the integrity of the markets and given the legalities related to the disclosure material information of the sort.

Q Now, once your earnings releases were drafted, what happened to them?

A Once they were drafted and approved, we would send them to the third party that was responsible for issuing those press release widely the wire.

Q Which newswires have you used in the past?

A Marketwired, PR Newswire. Those were the two that I'm recalling specifically.

Q Did you pay these newswires to distribute your press releases?

A Yes, we did.

Q Did you have an expectation of once you provided the press release to the newswire, it would keep it confidential?

A Yes.

Q Why use newswires?

A They are -- they are really built to widely disseminate information across the press. We would not have the capabilities necessarily, other than through an e-mail list or something similar to that. It was -- we were required by the SEC to publicly disclose in a manner that is reasonably likely to reach shareholders, and that was the most efficient way to make sure that that occurred.

Q Now you talked about public disclosure. Was there a requirement that the public disclosure be at the same time?
A Yes.
Q And why is that?
A It's to -- for the -- to make sure there's a level playing ground. There's -- I mean, it's -- you know, there's actually a regulation called fair disclosure so everyone receives the information and no one has that information before anyone else.
Q Did you learn at some point that the newswire you had been using to distribute Panera's press releases had been compromised?
A Yes. I actually think I read it through the news before. That was the first time I heard about it.
Q Do you remember which newswire it was, sitting here today?
A I don't remember which one it was exactly.
Q What did you do in response to learning this information?
A I think -- I think I reached out to -- or I know I reached out to our finance group, the folks who were responsible for reporting results externally, asked them if they had seen it; and then obviously wanted to make sure that there was nothing that we had done or was related to us that had been compromised to make sure that there was no data issue with respect to the information as we maintained it. That was

what I had thought about immediately, and it became pretty clear that this was something that happened outside of our reach.

MS. NESTOR: No further questions, Your Honor.

THE COURT: Any cross-examination for this gentleman?

MR. BRILL: Just a few. Thank you, Judge.

CROSS-EXAMINATION

BY MR. BRILL:

Q Good afternoon, Mr. DiPietro.

A Yes.

Q How are you?

A Good. Thank you.

Q Just a couple things.

You just told us that you found out that the newswire services had been intruded upon. I think you said you read it in the news.

A Yes.

Q Did you read it -- do you have any recollection as to the date? Was it in August of 2015?

A It was -- I believe that's around the time frame, yes.

Q Okay. And so is it fair to say that you had no knowledge that the newswire services that Panera Bread was utilizing had been compromised until that point?

A I don't know -- I know at one point we may have received

a call from somebody. I don't recall when that was that something had occurred, but I believe it was during that time frame when I read it online, what was the first time I had heard about it.

Q Okay.

Would it be fair to say, Mr. DiPietro, that as someone who is general counsel for Panera Bread, that you would -- in using newswire services, that you had an expectation that your data -- Panera Bread's data -- would be secure?

A Yes.

Q And would it be fair to say that if that data was indeed compromised, that would be something that you, as general counsel for Panera Bread, would want to know about?

A Yes.

Q You told us that there is a process in drafting press release earnings statements or earnings statement press releases, correct?

A Yes.

Q Yes.

And my question to you is that there comes a point where Panera Bread will submit that press release to a newswire service for distribution; is that a fair statement?

A Yes.

Q In the course -- in your involvement in that process of

drafting and submitting, do you -- have you had experiences where you have edited that press release once it's been submitted?

A I am aware where we have edited some of the text around potentially guidance for some of the information. The actual results, one, we wouldn't send them along until the actual -- in our EPS, the earnings per share number, was final.

Q But you would have the power, so to speak, to edit a document even after you submitted it to the press release.

A Until it was issued, yes.

MR. BRILL: Thank you so much, Mr. DiPietro.

THE COURT: Ms. Felder?

MS. FELDER: Yes, Your Honor.

CROSS-EXAMINATION

BY MS. FELDER:

Q Good afternoon.

A Good afternoon.

Q Just a few questions for you.

You testified that there is an earnings process that you undertake, correct?

A Yes.

Q And a part of that process is evaluating when to make information public in terms of the earnings calendar, correct?

A Yes.

Q And there are quarterly earnings calendar?

A They were -- yes. Quarterly, we would release earnings.
Q You would release it quarterly; however, investors know that the schedule is forthcoming, correct?
A Yes.
Q And because there is this process, and there's an earnings calendar, it's anticipated that your company would, at some point, publish the earnings reports.
A Yes.
Q And there's nothing about that calendar that is confidential, correct?
A The calendar itself, no.
Q There's nothing about the calendar that contains material information?
A Not that -- not the quarterly scheduled financial results, no.
Q And it is routine practice, you would say, or maybe you would agree, that investors in the investor community anticipates these earnings calendars in earnings reports, correct?
A Yes.

MS. FELDER: No further questions.

THE COURT: Thank you.

Anything further, Ms. Nestor?

MS. NESTOR: No, thank you, Your Honor.

THE COURT: Thank you very much. You may step down.

(Witness steps down.)

THE COURT: Folks, I have a little piece of business to attend to, so we're going to take an early lunch. We will resume at two o'clock. Enjoy your lunch. Do not discuss the case.

THE COURTROOM DEPUTY: All rise.

I'm just going to remind the jurors, please, to bring your notes with you.

(Jury exits.)

THE COURT: Have a seat, folks. We'll have this fellow in here momentarily.

(Short pause.)

(Juror enters.)

THE COURT: Good afternoon, sir. Have a seat.

Just for the record, your name is Lioz Hagler.

THE JUROR: Hagler, yes.

THE COURT: Ms. Mulqueen brought to my attention earlier this morning that there was something you wanted to speak to me about given the nature of the proceedings and the rules of the Court. This all has to be done in open court.

So what's on your mind?

THE JUROR: On Friday, unfortunately -- Thursday, rather, one of the breaks in the lunch -- not lunch break, the breaks in the jury room, somebody asked -- not asked, but it was informal discussion about -- well, informal discussion on

basically different things, and one thing, you know, vague and tangentially related to the case, but not exactly, like, you know, how many witnesses are we going to have today, you know, et cetera, et cetera, and I responded carelessly, unfortunately. My response to one of those inquiries -- one of those statements was -- this was -- sorry. Sorry. Take it back a step. This is when Mr. -- Igor -- the main witness. I'm drawing a blank now because I'm kind of nervous.

THE COURT: Mr. Dubovoy?

THE JUROR: Dubovoy. Thank you. Basically, I responded -- I'm trying to think exactly what my response was, but it was along the lines of -- well -- I don't want to misquote, since I'm, you know, here. It was along the lines of, he's the -- you know, the main -- the key prosecution witness, so we might be here -- he's probably going to be here all day, and that was pretty much it.

After I said it, I kind of, you know, realized that that was a very dangerous statement. How many people heard it? I don't know. I mean, we've had -- I won't say -- not to throw anybody else under the bus, but others have been saying, you know, small things. Even today, somebody mentioned something along the lines of, is it -- was the witness saying backslash versus regular slash. Now, is it -- does it impact the case? I can't say. But I understand that I made a very dangerous statement, and hopefully not fatal statement, on

Friday -- Thursday, and I just, you know, in all good conscience, I couldn't keep it from the Court.

THE COURT: Well, we're very grateful for that. That takes a little courage --

THE JUROR: Yeah, and I understand the ramifications, unfortunately.

THE COURT: They can be, as you said, deadly.

THE JUROR: Yes.

THE COURT: Let me ask you a couple questions.

That was the sum and substance of your comment, that we may be here all day?

THE JUROR: Well, the part that I felt uncomfortable in retrospect saying was the fact that it was the key prosecution witness, therefore, we'll be here all day. It wasn't that he would be here all day. It was the fact that I, kind of, referenced -- I felt uncomfortable, you know, again, after the fact that I said, you know, key prosecution witness, and I didn't want that, you know, that -- I was fearful that that could have been leading.

THE COURT: Identifying, in your view, as a key prosecution witness?

THE JUROR: The key prosecution witness, yeah, right.

THE COURT: Was there any discussion that that triggered?

THE JUROR: No, no. I don't think there was a reply from anybody. I don't know how many heard it either. That's the other thing.

THE COURT: Okay. And you don't recall how many people, if any, may have heard it.

THE JUROR: I would imagine, and honestly, you know, pondering this all weekend, I don't remember who put the initial query out there, so I would assume that person, you know, would have. I could see, you know -- I was toward the right side of the jury room -- the jury break room, so I would -- I could envision, you know, at least four or five people hearing it.

THE COURT: Well, it's apparent to me, Mr. Hagler, that you are, despite this misstep, you are scrupulously attempting to abide by my instructions. Please do better as we go forward.

THE JUROR: Understood.

THE COURT: I will make it clear to everyone that when I say no discussion about the case, I don't mean just about the merits of the specific testimony, any aspect of the case at all because it can trigger an exchange that would be unfortunate --

THE JUROR: Right.

THE COURT: -- and not called for.

So I thank you for your time. Let's close the book

on this, put it in the past, and please continue to abide by my instructions.

THE JUROR: Thank you. I apologize.

THE COURT: Thank you, sir.

THE COURTROOM DEPUTY: Okay.

(Juror exits.)

THE COURT: Unless anybody has any postmortems, I think we will leave it at that. See you at two o'clock.

MR. GOPSTEIN: Your Honor, just one --

THE COURT: One postmortem.

MR. GOPSTEIN: -- point with regard to this afternoon's witnesses.

THE COURT: Yes.

MR. GOPSTEIN: In their letter last night, defense counsel had requested a continuance for Thomas Carocci who -- I think he's our fourth scheduled witness for the afternoon, I'm not sure if he will get on any way, on the grounds that we have produced additional material over the weekend.

THE COURT: I understood your colleague here to say we're going to delay his appearance.

MR. GOPSTEIN: I've spoken with Ms. Whalen and Mr. Brill, and Ms. Whalen advised that she was going to defer to Mr. Brill. We were okay with delaying it, but I spoke with both of them in court today and Mr. Brill advised that he was fine with going forward with Mr. Carocci's testimony today if

we get to it, and so I wanted to put that on the record.

THE COURT: All right. Very well. See you at two o'clock.

MR. GOPSTEIN: Thank you, Your Honor.

(Lunch recess taken.)

A F T E R N O O N S E S S I O N

(The following takes place out of the presence of the jury.)

THE COURT: You've got a witness for us?

MR. TUCKER: Yes, the agent is getting him.

(Witness enters courtroom.)

THE COURT: Is this Mr. Ferguson?

THE WITNESS: Yes.

THE COURT: Come on up.

Have a seat.

(Witness takes the stand.)

(Jury enters courtroom.)

THE COURT: Please be seated, everyone.

Next witness please.

MR. TUCKER: Yes, Your Honor, the government calls Alistair Clark Ferguson.

(Witness sworn by the clerk.)

THE CLERK: Please state and spell your name for the record.

THE WITNESS: Sure, Alistair Clark Ferguson, A-L-I-S-T-A-I-R, F-E-R-G-U-S-O-N.

THE COURT: Mr. Tucker.

MR. TUCKER: Thank you, Your Honor.

(Witness takes the witness stand.)

ALISTAIR CLARK FERGUSON, called as a witness, having been

first duly sworn/affirmed, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. TUCKER:

Q Good afternoon, Mr. Ferguson.

A Hello.

Q Where are you employed, sir.

A I work at West Corporation.

Q What is West Corporation, very generally?

A West is a company that provides communication services quite broadly.

Q How long have you worked at West?

A Since April 2018.

THE COURT: Excuse me. Let's pull the microphone closer.

(Pause.)

Q My question was how long have you worked at West, Mr. Ferguson?

A Since April 2018.

Q Before that where did you work?

A I worked at NASDAQ Corporation.

Q When did you start at NASDAQ?

A February 2016.

Q And before you went to work at NASDAQ where did you work?

A I worked at Marketwired.

Q How did you come to work at NASDAQ from Marketwired?
A NASDAQ acquired Marketwired in February 2016.
Q When did you join Marketwired initially?
A In January 2014.
Q Does Marketwired still exist in some form today?
A The company does not, the technology has been integrated into NASDAQ and now West Services.
Q Focusing your attention of the period of time between January 2014 and February 2016 when you were employed by Marketwired, what were your responsibilities?
A I was responsible for the infrastructure and the security program, my title was VP Infrastructure and Chief Information Security Officer.
Q When you say VP --
A Vice president, I'm sorry.
Q Did you have employees under your supervision?
A Yes, approximately 35.
Q Where do you live, sir?
A I live in Ottawa, Canada.
Q What was Marketwired's general business?
A Marketwired provided press release services for clients.
Q What kinds of services?
A So, we help people get messages out about their earnings, about leadership changes, that kind of thing, so helping them meet their regulatory obligations and support communications.

Q And that was in part by distributing press releases?
A Yes.
Q Where was Marketwired based?
A Toronto, Canada.
Q Did Marketwired have any competitors or peer companies that offered similar services?
A So, Business Wire and PR Newswire would be a couple in North America, yeah.
Q Did Marketwired specialize in any particular sector of businesses for issuing press releases?
A No, it was quite broad across quite a number of sectors.
Q How did Marketwired's customers provide press releases to Marketwired for distribution?
A So, customers would access our service through a browser, connect over the internet to our portal. They'd log in, authenticate themselves with an ID and a password and then once they were in the portal they would provide the information when they wanted the release to be published and the things like the title, headline and the body of the release.
Q All right. Just to unpack that a bit, was that portal referred to as the CS3 portal?
A Yes.
Q Please tell the jury what the CS3 portal was?
A CS3 is the name of the press release services which we

provided for clients in the U.S. region.

Q Now, you testified that Marketwired employees had to log in to the CS3 portal before they could upload press releases?

THE COURT: Did you say employees?

Q I'm sorry, Marketwired customers had to log into the Marketwired portal before they could upload press releases?

A That's correct.

Q They'd need a user name and a password?

A Yes.

Q And the different preferences that Marketwired customers were able to choose when they uploaded press releases, one of those was when a press release would be published?

A Yes.

Q And were they also able to select how the press releases would be distributed?

A Yes. So, they would select from a variety of end points, typically under their contract they would have predetermined a group of end points, but the press releases would go out to end points which are media channels and then out through email and out through an investor relations website.

Q Just so it is clear, those end points could include news websites and news publications among other things?

A Yes.

Q And users of the CS3 applications could also make formatting choices about the press releases?

A Yes.
Q Once they'd done all that, what was the next step in the upload process?
A So, in interacting with portal they'll upload the body of the content and then they'll click confirm and that would signal our editorial team that a new release had been submitted and required attention.
Q And what would happen after that?
A So, our editorial team would review the press release for any kind of spelling mistakes, incorrect information, formatting issues; with things like financial tables we wanted to make sure that it was really clear in the final product.
Q Would the Marketwired editorial staff make substantive changes to press releases sometimes?
A Sometimes but it would be -- once their job was done it would be returned to the client for approval.
Q If substantive changes were made, how did that process work?
A They would edit the content within the web portal and save the changes and return a proof to the client for review.
Q Would those edits be made in conjunction with the client?
A Yes.
Q Once a press release was ready to be released and the appointed time of distribution arrived, what happened then, Mr. Ferguson?

A At the appointed time the unencrypted information would be sent out over the media channels to each of the end points that were selected for the release.
Q So, at that point Marketwired would distribute the final press releases?
A Yes.
Q Is that right?
A Yes.
Q Was it important for Marketwired to ensure that the draft press releases it received were kept confidential between that initial time of upload and the appointed release time to the public?
A Yes.
Q Why?
A It's part of the confidentiality agreement that we had with the customers that their information would be maintained confidential until the appointed time of release.
Q Why was that important?
A It is important for the clients to have their information disclosed simultaneous to investors and shareholders under regulatory laws and so that's why we were a trusted provider of the service in meeting those obligations.
Q Was that confidentiality incorporated into the end user agreements that Marketwired had with its customers?
A Yes, it was.

Q Mr. Ferguson, in that pile in front of you are some documents that have been marked for identification as Government's Exhibits 831 through 842. Do you see that pile, sir?
A Yes.
Q What are these documents generally?
A These are copies of press releases that were submitted into our CS3 system.
Q So, these are the draft press releases --
A Yes.
Q -- as initially uploaded by Marketwired employees to Marketwired system?
A By customers into the CS3 system, yes.
Q And did you provide those to the government at the government's request?
A Yes, I did.
Q And how did you go about extracting or obtaining these draft press releases from the Marketwired systems?
A So, we -- the information is maintained in a database system and so we applied a query on the specific information that the government requested and extracted the files, provided them to you.
Q Are these true and accurate copies of those press releases from the Marketwired archives, Government's Exhibits 831 through 842?

A Yes, they are.

MR. TUCKER: Your Honor, the government moves to admit Government's Exhibits 831 through 842.

THE COURT: Any objection?

MS. BRILL: There is, Your Honor. May we have voir dire or explain at the bench?

THE COURT: Well, if the voir dire is related to your objection --

MS. BRILL: The objection is it is being admitted for what they were described to be, yes.

THE COURT: I think you better come on over.

(Continued on next page.)

(The following takes place at side-bar.)

THE COURT: Yes, ma'am.

MS. BRILL: Before I start, that similar pile is in front of the witness?

MR. TUCKER: Correct, identical.

MS. BRILL: Your Honor, I will believe that the government just got from the witness that these will be the press releases as uploaded by the client. In addition, the government will from this witness elicit -- hopes to elicit foundation for a chart that will include a couple of items; one of the items will be the time that the press release was released to the public but one of the items will also be the time that the press release was uploaded by the client.

So, there will be a column for the time it was uploaded, there will be a column for the time it was released, there will be a column of the press releases that were uploaded and there will be a column of the press releases that were released. And so it is -- but I believe that there are indications from the discovery that we have gotten and from my study of those documents that these documents in front of Your Honor are not copies. I understand that's what the witness said but there are indications that they may not be copies of what was uploaded by the client at the time that's going to be on the chart that the government seeks to admit.

THE COURT: They are not what he said they were?

MS. BRILL: They're not what -- they may not be -- let me put it this way, they may not be what the government elicited they were which is the press releases that were uploaded at the particular time that's going to be on the chart.

THE COURT: Well, ask him, you can have some voir dire.

MS. BRILL: Some voir dire.

(End of side-bar.)

(Continued on the next page.)

(In open court.)

THE COURT: Go ahead, Ms. Brill.

MS. BRILL: Your Honor, can I go to the podium?

THE COURT: Of course.

MS. BRILL: Before I get to the podium can I have Exhibit 405 that's already in evidence?

(Pause while counsel confer.)

VOIR DIRE EXAMINATION

BY MS. BRILL:

Q Mr. Ferguson, in front of you is a pile of documents numbered 831 to 842, is that right?

A Yes.

Q And you've testified in answers to the prosecutor's questions that those are the press releases as uploaded by the client, right?

A That's correct.

Q When they went to the portal and said confirmed?

A Yes.

Q And those are maintained by your company, whether it was Marketwired or NASDAQ or West as it is now; is West also a wire company?

A We are, yes.

Q All right. So, I want to show you what's already been marked as Exhibit 405 and that is, as you can see, I'm sure there's a way to make it a little bit smaller --

MS. BRILL: Everybody can see this, it is an exhibit.

THE CLERK: Okay.

Q As everybody can see, this is a TIBCO press release; is that what it looks like from the top?

A Yes.

Q And on the bottom there's some markings?

A Yes.

Q And that looks like something that came from TIBCO perhaps that's on the document as it is uploaded to your company?

A It looks like the name of the document as it was printed.

Q It looks like the name of the document as it was printed?

A The string of characters I'm seeing here looks like a Word document name of the file.

Q But does it look like it was part of the document?

A That is -- what I mean is I think it looks like in the way that that file was generated that it is the name of the file of the document.

Q And that document -- Exhibit 405 is a document that was extracted from a computer in the Ukraine, that is what Exhibit 405 is, and those markings are on the bottom as highlighted by the government.

MR. TUCKER: Objection, Your Honor.

THE COURT: Can we have a question?

Q Can you look at Exhibit 831.
A Yes.
Q Do you see those same markings at the bottom of Exhibit 831?
A Yes, it is a TIBCO press release.
Q And you see the same markings on the bottom?
A Yes.
Q Now, look at Exhibit 832, that's an exhibit from Edwards Corporation or some -- Edwards something, right?
A Yes.
Q And that exhibit does not have the markings on the bottom?
A Right.
Q What about that exhibit indicates to you that it was uploaded?
A The fact that we've taken it out of our system from the database in the area where the client had uploaded it is how this is -- how I can verify that this is from the client.
Q All right. So, you took it out of the area where things are uploaded?
A Yes, the database, CS3.
Q I want you to look at one more document and then I do just have a very few questions about that.
So, we see from a TIBCO document, from the area that it was uploaded that there's markings on the bottom, you see

from the Edwards document that there aren't markings on the bottom when it is uploaded; can you look at Exhibit 840.

A Got it.

Q 840 is also a TIBCO press release, right?

A Yes.

Q Different quarter, different contents, different press release, right?

A Yes.

Q But that has no markings on the bottom, right?

A That's right.

Q So, for some reason TIBCO uploaded one with markings and one without markings?

A Yes.

Q You talked about how things get changed in your database; do you maintain those changes in another area?

A The changes are maintained in the CS3 database itself.

Q Is the CS3 database what you searched in order to come up with documents 831 to 842?

A Yes, it is.

Q So, you went to the CS3 -- there's no other database, it's just the CS3 database?

A That's correct.

Q And they have the documents that are uploaded and the documents that are edited and then resubmitted, for lack of a better word?

A Yes.
Q And there's no way to distinguish between which documents were uploaded and not changed and which documents were uploaded and changed in the CS3 database, correct?
A The system itself has an audit log which maintains the changes so we have a trail of information indicating when information in a press release is changed.
Q So, when did the information on the press release that's exhibit for identification 831 change and the markings were removed?
A After the client uploaded the document and they clicked confirm the editorial team would have done the cleanup on the document.
Q And then would it not have replaced the document in this CS3 database, as you just testified?
A The document would have been adjusted, it would not have been replaced. There would be a new version of the information maintained in the database.
Q Would the old version of the information be maintained in the database?
A Yes.
MR. TUCKER: Your Honor, could we have a breach side bar?
THE COURT: I don't think it is necessary.
Do you have anything else?

MS. BRILL: Hold on. (Pause.)

Q The TIBCO press release for the quarter that's in front of you that's marked as exhibit for identification 831.

A Yes.

Q How many of those press releases are in the CS3 database -- would be in the CS3 database?

THE COURT: That's not proper voir dire, with all due respect, Ms. Brill.

I'm going to receive the documents. Let's go. 831 to 842 now in evidence.

(Government Exhibit 831 through 842, were received in evidence.)

MR. TUCKER: Thank you, Your Honor. May we publish?

THE COURT: Go ahead.

DIRECT EXAMINATION

BY MR. TUCKER:

Q So, Mr. Ferguson, looking at 831 for a minute, just so it is clear for the record, the documents that you, and I guess West today, but were extracted from Marketwired systems, those were provided in Word document form right?

A Yes.

Q So a .doc or .docx, right?

A That's correct.

Q They certainly weren't provided to the government printed out with Government's Exhibits?

A No.
Q Now, each one of those Word documents, electronic documents that was provided to the government had a file name associated with it, right?
A Correct.
Q Was this the file name associated with this particular TIBCO press release?
A That's my understanding, yes.
Q And that's based on your review and what you produced, right?
A Yes.
Q So, these other files now in evidence, 832 for instance, it would have a file name also, right?
A Yes.
Q We just didn't label it at the bottom?
A Correct.
Q So, all you can tell from this particular footer is that this was the file name associated with this particular draft press release, is that right?
A Yes.
Q Thank you.

Mr. Ferguson, in front of you is a pile of documents -- and Ms. Mulqueen will bear with me for a moment -- these documents have been marked for identification as Government Exhibits 4541, 4542, 4543, 4544, 4551, 4554,

4592, 4594, 4620, 4625, 4674 and 4675; is that right, Mr. Ferguson?

A Yes.

Q And you've had a chance to review those prior to your testimony here today?

A I have.

Q What are these documents generally?

A These documents are the final releases on behalf of our clients.

Q Are these printed off of Marketwired's website?

A Yes.

Q And did you personally print these and mark these?

A No.

Q Did you personally verify that these are in fact the final press releases as stored in the Marketwired website?

A I did.

Q And Mr. Ferguson, these press releases reflect distribution dates of the final press releases?

A Yes.

Q Those reflect distribution dates and times?

A They do.

Q Does Marketwired or its subsequent companies, do they edit the press releases on the Marketwired system after they are distributed?

A No.

Q So, if these were printed out within the last few weeks, you would expect these to be the same press releases as they were distributed during their distribution times on the documents?

A Yes.

MR. TUCKER: Your Honor, the government moves to admit that series of exhibits. I can read them again if the Court wishes.

THE COURT: I think -- Ellie, you have them?

THE CLERK: Yes, I believe I do.

THE COURT: Madame?

MS. BRILL: To these documents, no objection, Your Honor.

THE COURT: Received.

(Government Exhibit 4541, 4542, 4543, 4544, 4511, 4554, 4592, 4594, 4620, 4625, 4674, and 4675, were received in evidence.)

MR. TUCKER: Thank you, Your Honor.

May we publish?

THE COURT: Go right ahead.

Q All right. So, once again, Mr. Ferguson, this was a series of final press releases. I am just going to show you one example. This is what's in evidence now as Government's Exhibit 4674, is that right?

A Yes.

Q And is this final press release that corresponds to what's in evidence as Government's Exhibit 831?
A Yes, it is.
Q So, it is the same date of distribution, June 28, 2012?
A Yes.
Q Same headline?
A Yes, it is.
Q So, that series of second documents, those are the final press releases as issued from the draft press releases we admitted a moment ago?
A That's correct.
MR. TUCKER: Just for the witness, Ms. Mulqueen.
Q I'm showing the witness what's been marked for identification -- it is a CD marked Government's Exhibit 802.
Do you recognize that CD, Mr. Ferguson?
A I do.
Q What is it?
A This is the CD containing the files that we provided to the government.
Q All right. What kind of files are on Government's Exhibit 802?
A It would list all of our press releases from the time of 2009 through 2014 and the other documents that we've provided.
Q Does it include submission dates and times and distribution dates and times for all the Marketwired's press

releases during that period?
A It does.
Q And did you personally extract all that data from Marketwired systems?
A I supervised it and ensured it was correct.
Q Are these records kept by the Marketwired in the ordinary course of business?
A They are.
Q How are they used by Marketwired?
A It's a history of our service to the client, so it would be used for billing purposes as well as on request if there was any confusion around what we -- how we had handled the information, it would be available.
Q Is this data populated in Marketwired systems through a manual or an automated process?
A Through an automated process.
Q Does that occur close in time to the events being described?
A Yes.
Q And you personally verified the data on 802?
A I have.
Q Do you recognize your signature and the date on it?
A Yes.
MR. TUCKER: Your Honor, the government moves to admit Government's Exhibit 802 and its contents into

evidence.

THE COURT: 802.

MS. BRILL: No objection.

THE COURT: Received.

MR. TUCKER: Thank you, Your Honor.

(Government Exhibit 802, was received in evidence.)

Q One question before we move on, Mr. Ferguson. The data that's stored on 802, is that in Pacific time?

A It is.

Q Okay. Now, just for the witness, I'm going to show the witness what's been marked for identification as 802-2.

THE CLERK: 802-2?

MR. TUCKER: Yes.

Q Do you recognize this chart, Mr. Ferguson?

A I do.

Q Did you make this chart?

A I did not.

Q Did you personally verify the information it contains?

A I did.

Q Is this derived from what's now in evidence as Government's Exhibit 802?

A It is.

Q Is this a small excerpt of the data that's on there?

A That's correct.

Q Just so it is clear, have the times in this excerpt been

harmonized to Eastern time?

A Yes, that's correct.

MR. TUCKER: Your Honor, the government moves to admit Government's Exhibit 802-2 into evidence.

THE COURT: Any objection?

MS. BRILL: Only subject to our previous objection to the admission in evidence of the documents that are referenced on the chart.

THE COURT: I see. Subject to that, 802-2 is now in evidence.

(Government Exhibit 802-2, was received in evidence.)

MR. TUCKER: Thank you, Your Honor.

May we publish?

THE COURT: Please.

MR. TUCKER: Okay.

Q So, now that the jury can see, Mr. Ferguson, so is this the type of data that is stored on the CD now in evidence as Government's Exhibit 802?

A Yes, it is.

Q So, it includes information like the distribution date and time and the submission date and time?

A That's correct.

Q Just working from left to right, can you explain to the jury what the significance is of the RowNum column is?

A Sure, that's just a row in the database system where this record is provided, extracted from.
Q PRID, what's that?
A It's the press release ID.
Q Is that a unique identifier assigned by Marketwired?
A By the system for this release.
Q What's release type?
A That's the title that the client would have provided for the release.
Q And the distribution date?
A It is the date and time that the client selected for the release to be distributed.
Q And the source?
A The source is the name of the company that we're providing the service to.
Q Just so it is clear, Mr. Ferguson, that is the distribution date and time selected by the user and that is the actual distribution time?
A Yes, it is.
Q CPID, what's that?
A It is an internal identifier for the company that we're servicing, so in this case 126798 connects to TIBCO
Q Company name?
A In some cases the companies might have a department within so we stored that separately in the database.

Q Submission date?
A That's the point in time when they uploaded the file ahead of clicking confirm.
Q And so it is clear, Mr. Ferguson, these last two columns, that's not Marketwired data, right?
A No, it is not.
Q Those are just corresponding exhibit numbers; is that right?
A That's correct.
Q So, at this point this chart reflects the draft press releases and the final distributed press releases that you just authenticated?
A That's correct.
Q And, again, that just a small fragment of the data from 802?
A Correct.
MR. TUCKER: Just for the witness, Ms. Mulqueen. I'm showing the witness what's been marked for identification as Government's Exhibit 4627.
Q Do you recognize that document, Mr. Ferguson?
A I do.
Q What is it?
A There is an Oracle final press release.
Q Is this copied from the Marketwired website?
A Yes, it is.

Q Is this a fair and accurate copy of a final press release that was distributed as shown here?
A Yes, it is.
MR. TUCKER: Your Honor, the government moves to admit Government's Exhibit 4627 into evidence.
THE COURT: 4627, all right, just checking my notes. , any objection?
MS. BRILL: No objection.
THE COURT: 4627 in evidence.
(Government Exhibit 4627, was received in evidence.)
MR. TUCKER: May we publish?
THE COURT: Go ahead, yes, sir.
Q So, for the record, Mr. Ferguson, this is an Oracle press release dated December 18, 2013, is that right?
A That's correct.
Q And the distribution time on this was 16:04 east coast time or 4:04 p.m. east coast time?
A Yes.
Q Now, Mr. Ferguson, I'm going to show you what's in evidence as Government's Exhibit 323. Have you seen that document prior to your testimony here today?
A Yes.
Q How did you see this document?
A The government provided it to me for review.
Q Based on your -- well, my first question, Mr. Ferguson,

is have you looked at the text in Government's Exhibit 423?
A Yes, I have.
Q And does this text correspond to the distributed press release now in evidence, 4627?
A It does.
Q It's excerpt?
A It is an excerpt, I found it matching on both page four of the --
Q Directing your attention to page four, just to look for a couple of examples, there's some text here -- tell me if I read this right: As of November 30th, 2013, approximately $2 million in estimated revenues related to hardware systems support contracts.
THE COURT: I think you may have misspoken, I think you meant 323, not 423, correct?
MR. TUCKER: I apologize, Your Honor, this is, for the record, 323-A1.
Q And that text I just read, direct your attention back to 4627 which is in evidence, does that correspond to this text here: As of November 30th, 2013, approximately $2 million in estimated revenues related to hardware systems support contracts?
A That's correct.
Q And there's also references to Oracle Corporation, Q2, 2014, year-to-date financial results condensed?

A Yes.
Q Does that correspond to the fifth page of 4627, that same text?
A Yes, it does.
Q And the numbers in the table, in 4627, do you see those numbers in a different format but they're in 323-A1?
A Yes, it's sprinkled in, it is not formatted well but it is in the section just under the title.
Q Just for the record, you tapped on your screen basically in the middle of this screen shot; is that right?
A Yes.
Q Mr. Ferguson, based on your knowledge of Marketwired systems, does this appear to be a final distributed Marketwired press release that's in Government's Exhibit 323-A1?
A It looks like the final release but it's not the final release because it's not sort of containing fully human readable, the fact that it's not formatted well and it has a bunch of dashes suggests it has special characters in it.
Q When you say "special characters," what do you mean by that?
A More system characters such as we would store it when it is in the database.
Q In Marketwired's database?
A Yes.

MR. TUCKER: Just for the witness, Ms. Mulqueen.

THE CLERK: Just for the witness.

MR. TUCKER: Thank you.

Q I'm showing the witness what's been marked for identification as Government's Exhibit 802-1.

A Yes.

Q Which is a two page document. Mr. Ferguson, is this an excerpt from all of the uploaded data stored on that CD, Government's Exhibit 802, corresponding to the Oracle press release you were just testifying about?

A It is.

Q Is the first page as it appears in the database and the second page harmonized to east coast time?

A Yes, that's correct.

MR. TUCKER: Your Honor, the government moves to admit 802-1 into evidence.

THE COURT: Any objection?

MS. BRILL: No objection.

THE COURT: 802-1 in evidence.

(Government's Exhibit 802-1 received in evidence.)

MR. TUCKER: May we publish, Your Honor?

THE COURT: Go ahead.

Q So, turning to the second page of 802-1, this reflects a submission time of 12/17/2013 at 10:34 a.m., is that right?

A That's correct.

Q And distribution date and time of December 18th, 2013 at 16:04 p.m. east coast time; is that right?
A Yes, that's correct.
Q And that corresponds to what we see on the face of the final press release, 4627?
A Correct.
Q December 18, 2013, 16:04 east coast time; is that right?
A Yes.
Q Mr. Ferguson, please remind us when you came to work for Marketwired initially?
A January 2014.
Q What led to your hiring there, if you know?
A The company had experienced some pretty significant systems problems, breaches, and as part of the strengthening the program they hired me as the Chief Information Security Officer.
Q Did Marketwired make efforts to improve its cyber security posture?
A Significant.
Q Even with those efforts did Marketwired continue to be the target of malicious cyber activity after you joined the company?
A Yes.

MR. TUCKER: No further questions, Your Honor.

THE COURT: All righty.

Ms. Brill?

MS. BRILL: Yes, Your Honor.

CROSS-EXAMINATION

BY MS. BRILL:

Q When were you acquired by NASDAQ?

A Marketwired?

Q When was Marketwired acquired by NASDAQ I should ask?

A February 2016.

Q And was a disclosure made to NASDAQ that the systems had been severely compromised, do you know?

A Yes.

Q Yes, you know and, yes, the disclosure was made?

A Yes.

Q So, referring again only to the uploaded press releases, not to the distributed press releases.

A Okay.

Q Is it your testimony that you maintain all of the uploaded press releases as uploaded?

A That's correct.

Q And do you maintain separate copies of all of the uploaded as edited?

A Yes, that's what becomes the final.

Q So, there are several different versions maintained in your system, the uploaded version, any edits that might be made and the final distributed version?

A Yes.
Q You have all of those in your system?
A Yes.
Q So, let me just talk a little bit about the editing that does take place. I mean you spoke about the fact that it is handed over to your editors or your editorial team, right, once it is uploaded and editing can be as simple as formatting, right?
A Correct.
Q It could be as simple as removing the markings that I was talking about earlier, right?
A Yes.
Q And it could also be a little more complex like changing words, right?
A Yes, that's true.
Q Changing numbers?
A Yes, that's correct.
Q Changing paragraphs?
A Yes, under the client's direction.
Q And under the client's direction you could also add and subtract pages, right?
A Yes.
Q There's a system in place, there's a protocol in place for the press releases to be altered even after they're uploaded on your portal, right?

A That's correct.
Q I'm going to talk a little bit also about -- and when those documents are edited, nothing changes about the uploaded time?
A Not the submission time, that's maintained from the original submission.
Q Even after you send it over to the client for an okay and bring it back?
A Submission time --
Q Yes, for distribution?
A That's correct, it stays the same.
Q So, you spoke a little bit about confidentiality and you're aware, are you not, that there's a -- do you have a relationship with your clients that requires that the documents be kept confidential, your company has that relationship, right?
A That's correct.
Q And it is important for the company to keep those documents confidential?
A Yes.
Q It is important for Marketwired and it is important for the corporation, right?
A Correct.
Q And that's the service that you offer, that's what the clients contract?

A Yes.
Q And part of keeping the documents confidential you would agree is keeping the system secure, right?
A Correct.
Q So, if the security is breached, then Marketwired, the company is not fulfilling its obligation to keep the documents confidential, would that be fair to say?
A Correct.
MS. BRILL: I don't have any further questions.
THE COURT: Thank you.
Anything else?
CROSS-EXAMINATION
BY MS. FELDER:
Q Good afternoon, Mr. Ferguson.
A Hello.
Q I'd like to show you what was previously admitted as Government Exhibit 323-A1.
A Yes.
Q You testified that the government provided you with this document, correct?
A Yes.
Q When were you provided with this?
A Within the last week.
Q Did you ever see this document or text prior to the government showing it to you?

A No.
Q Did you review the CS3 portal to compare this document to whatever is in the portal?
A I compared it to the final release, I didn't compare it to what was in the portal.
Q You testified that your clients would upload information to that portal, correct?
A Yes.
Q And they would upload the body content of the press release, correct?
A Yes.
Q One other question, do you know the source of this text?
THE COURT: I'm sorry, I didn't hear the end of that.
Q Do you know the source of this text?
A The source of the text?
Q Yes.
A I only know that it looks like the other document, I don't know where it came from.
Q You have no personal knowledge of where it came from, correct?
A No.
Q Or what computer it was on, correct?
A No.
Q And it's not anything similar to what you've seen in the

portal, correct?

A I didn't look in the portal for this document.

MS. FELDER: No further questions.

THE COURT: Thank you.

Anything else?

MR. TUCKER: No, Your Honor.

THE COURT: Thank you, Mr. Ferguson. Appreciate it. Step down.

Next witness.

(Continued on next page.)

MR. TUCKER: The Government calls James Gimbi.

(Witness takes the witness stand.)

JAMES GIMBI, called as a witness, having been first duly sworn/affirmed, was examined and testified as follows:

THE WITNESS: I do.

COURTROOM DEPUTY: Please have a seat state and spell your name for the record.

THE WITNESS: My name is James Gimbi, J-A-M-E-S, G-I-M-B-I.

MR. TUCKER: May I inquire, your Honor?

THE COURT: Yes, sir.

DIRECT EXAMINATION

BY MR. TUCKER: :

Q Good afternoon, Mr. Gimbi. Where are you employed, sir?

A I work for the United States Senate.

Q What do you do for the Senate?

A I am a cyber security legislation policy adviser.

Q What does that mean to be a cyber security legislation policy adviser?

A Sure. So my role is to help a Senator deal with cyber security issues as they come up and draft legislation direction for potential future changes.

Q How long have you been working in the Senate?

A Since January.

Q How long is your fellowship?

A The fellowship lasts until December 31, 2018.
Q Where were you employed prior to the Senate?
A Mandiant.
Q What is Mandiant?
A Mandiant is a cyber security consulting firm. And the company does a range of cyber security professional services, consulting, specializing most specifically in incident response and forensic analysis.
Q When you say incident response, what do you mean by that?
A Incident response is the practice of helping an organization when a company or Government agency is dealing with a breach, a hacker, once they have found a way into the environment. So that might include first identifying the full scope of an incident, as well as developing a plan to extract the attacker from the environment and prevent them from coming back again.
Q What is your educational background?
A I went to the Rochester Institute of Technology. And had a, received a Bachelor's degree with honors in information security and forensics.
Q Have you received specialized training in information security and forensics?
A I have.
Q Please tell the jury a little about that.
A There was the Bachelor's degree, which again focused

heavily on analysis, techniques and procedures. As well as evidence handling and processes that would help surrounding the delivery of an incident response engagement.

Since working at Manhattan I have taken several classes, as well as taught several classes, for federal law enforcement and others.

Q Focusing on the teaching for a moment, please tell the jury and the Court a little about the type of classes you taught?

A Sure. So the classes I taught were analysis techniques, forensic methods and offensive techniques for corporate clients, new consultants at the company, conferences and federal law enforcement.

Q During your time at Mandiant, about how many different clients have you provided cyber forensic and information security consulting services?

A Somewhere in the order of 95.

Q What was that time period?

A From 2012 June 2012 until just this last January.

Q Are you being paid in connection with your testimony here today, Mr. Gimbi?

A I'm being reimbursed for travel; aside from that, no.

MR. TUCKER: At this time the Government offers Mr. Gimbi as an expert in information security, computer forensics and cyber incident responses.

THE COURT: Either counsel wish to exam at this point?

MS. BRILL: Your Honor, if I could just say, is this witness going to be giving an opinion?

THE COURT: He's being offered as an expert witness, I assume he is.

MR. TUCKER: Yes.

MS. BRILL: There is no voir dire, your Honor. That was my only question.

THE COURT: Very well.

MS. FELDER: No objection, your Honor.

THE COURT: Ladies and gentlemen let me interject for just a second. You heard a term I myself don't generally use, that of opinion witness -- of an expert witness, excuse me. This has nothing to do with this gentleman. I would say this no matter who was called and proffered to the jury as a so-called expert witness.

You are the judges of facts, all facts. Even facts about which an opinion or expert witness will testify to. If you believe that the evidence does not support an opinion expressed, you're free to reject it. If you think the background or experience of an expert witness is not sufficient to support an opinion or opinions expressed by that witness, you're free to reject it. If you think there is other evidence in the case that convenes what an opinion or

expert witness has to say, you're free to reject.

Which is why I choose the label opinion witness rather than expert witness so that the jury is not in any way confused that on all facts in dispute, all facts, you the jury are the judges of those facts. Okay. So bear that in mind.

As I said, I say this to you regardless of who the witness is. I refer to him as an opinion witness, lawyers will often hear, as you've already heard, refer to them as expert witnesses. But you're the expert. You're the ultimate finder of all facts. Okay. Please continue.

MR. TUCKER: Thank you, your Honor.

BY MR. TUCKER:

Q Mr. Ferguson, I want to return your attention to June 2013. Did there come a time when you were part of a Mandiant incident response team that worked in engagement at Marketwired?

A Correct. My last is Gimbi, yes.

Q I'm sorry, Mr. Gimbi. I apologize. Mr. Gimbi.

THE COURT: You have to correct that incident, didn't you?

Q My apologies, Mr. Gimbi.

What was your understanding of the events that led up to that engagement at Marketwired?

A My understanding is that the Secret Service had notified Marketwired that there had been a breach. They had advised

that they seek expert assistance to deal with the breach.
Q Did you have to travel anywhere as part of your work in that engagement?
A I did. I went to Toronto twice.
Q All together, how long did you work on that project?
A It was about two weeks on site, and another I would say four to six weeks offsite.
Q Did you have anybody else with you from Mandiant when you responded to Marketwired?
A Yes.
Q Who was -- approximately how many other people were with you?
A Two other consultants on the case.
Q When you arrived at Marketwired, what were your objectives?
A The objectives were first to understand the full scope of the incident. And the second objective was to remove the attacker from the environment. The third was to prevent attacks from happening again.
THE COURT: Would you move a little closer to the microphone.
THE WITNESS: Is this better?
THE COURT: We'll see.
Q Mr. Gimbi, could you just restate your answer, what your objectives were, I couldn't hear?

A The objectives were to identify the full scope of the breach; remove the attacker from the environment; and third, prevent the similar attack from happening again.
Q So focusing on the first role, identifying the full scope of the incident, what does that mean?
A Full scope means we're looking to understand everything that the attacker had done in terms of every system that they had interacted with and ideally all the data that they would have had accessed to and were removed from the environment.
Q And removed from the environment, what does that mean?
A To copy data from a victim network work onto some other network, often for some other use distribution or re-sale.
Q When you say remove the attacker from the environment?
A Excuse me -- yes.
Q What do you mean?
A That would mean to take away whatever means of access that they have. If they are getting in through the back door, we close the back door and lock it.
Q When you conduct an incident response in a case like this, what is the pace or level of urgency?
A The pace depends very much on a few different factors. Most importantly the type of attack they are, what you're dealing with and the risk tolerance of the client. You would treat, for instance, when you talk about type of attacker a nation state espionage organization is very different than how

you treat an organization that was actively stealing money at a very high rate from the organization.

Q How would those differ?

A When you're dealing with an intelligence agency or an agent of a nation state, you generally don't want them to know that you know that they are there until you fully understand everywhere they are so you can remove them from the environment faster than they would be able to respond and dig deeper in.

When you're dealing with a financially motivated attacker, the incentives change. You want to do everything you can to stop the loss of capital as soon as you can.

Q What was the tempo like for the Marketwired engagement?

A A little bit in between.

Q Tell the jury the general methodology that you and your team employed at Marketwired?

A You take whatever facts you have available to you. In this case I believe we had a few different IP addresses that were reported as malicious. As well as a sea full of what we were told was evidence collected by the Secret Service. And we look to see if anything would have lined up with those pieces of evidence could be found in artifacts in Marketwired's actual environment.

From there you follow the leads. So you work with this one fact that you have, timeline around that, look at

what happened on the system at that point, learn more about the scope, if they had moved laterally, moved to another machine. You would complete -- or excuse me, continue that process until you stop finding new things essentially.

Q What kind of evidence did you obtain and review in your work at Marketwired?

A The two primary sources of evidence were log files from various services and file system information from forensic images.

Q What are log files?

A Log files are computer files, often flat text files, that are dynamically generated; that is to say, actively added as a computer does what a computer would normally do, different types of logs for different sources of events.

You may have a log every time somebody logs into a computer. For instance, every time you sign into your computer your computer keeps track of what you did, what the username was, whether or not it was successful, and stores that for later inspection.

Q So those are records of the activity that the system is undergoing?

A Correct.

Q You mentioned that you also examined forensic images, please explain what you mean by that?

A Forensic image is a bit for bit copy of a hard drive of a

computer.

Q What kind of thing to us look for when you look at forensic imagings?

A When you're looking at a forensic image, you're generally trying to understand what an attacker actually performed while they were effecting or on you might say a system. So you can find evidence of them creating, removing files, collecting files. You could find evidence of what, potentially evidence, of what directories they had seen, commands that they had run, and other such things.

Q When you do a review of a forensic image are you looking for malware?

A Yes.

Q What is malware?

A Malware is software that is designed for some malicious purpose, hence malware. Malware with a back door that lets you have access to a machine that you're not supposed to have access to. It can be a key logger, which tracks everything that person types, or it can be something like ransomware.

Q In your review of the web logs from Marketwired's systems, did you see evidence of malicious activity?

A Yes.

Q Did you also see evidence of malware on Marketwired systems?

A Yes.

Q By the way, you've been talking about reviewing forensic images; is that right?
A Yes.
Q Did you look at the actual machines that were operating Marketwired systems while they were online?
A No.
Q Why the images?
A An image is for the purpose of being forensically sound. If can you get an image of a computer -- if a computer is on and active in production mode, the contents of the hard drive are constantly changing. Most digital artifact, just like real artifacts, have a life span of sorts. Like a foot print in mud is somewhat ephemeral, weather can make it go away. So what we're basically doing is taking a cast of the system so we know actually what was on at the time of analysis, or time of collection rather.
Q Based on your overview of the forensic images and logs, were you able to determine when the malicious activity targeting Marketwired systems began?
A Yes.
Q When?
A February of 2010.
Q Did that malicious activity occur on and off after that during at arrival of the Mandiant team?
A Yes.

Q You arrived in June of 2013?
A Correct.
Q You testified that the earliest evidence of malicious activity was in February 2010. In your experience, Mr. Gimbi, do malicious cyber attackers sometimes take measures to remove or conceal evidence of their activities?
A Yes.
Q What kinds of measures?
A Well, you would most commonly see an attacker delete or modify log files. Probably the lowest hanging fruit, we call an anti-forensic.
Q You said lowest hanging fruit?
A Lowest hanging fruit, I guess easiest thing to do with the highest impact.
Q That was anti-forensic activity?
A Yes.
Q What is the point of modifying or deleting log files?
A The two big points would be first to slow down an investigation generally. And the second would be to obfuscate attribution attempts, make it harder to work.
Q When you say attribution attempts, figuring out who the attacker is?
A Yes.
Q Were you able to determine how the attackers gained access to Marketwired systems initially?

A Yes.
Q What did they do?
A They used a technique known as SQL injection or SQL injection on a front Internet based Marketwired application.
Q Briefly, remind us what SQL injection is?
A Taking a quick step back, SQL is a database, common database. A database is like a big filing cabinet, lots of drawers in it, and in the drawers are folders containing data. Similarly, a database is a series of tables that contain rows and columns full of information.

So a SQL injection attack is when you find a way to ask for information from one of those digital filing cabinets that you should not get your hands on, that you should not have access to.
Q Do SQL injection query sometimes allow attackers to extract information?
A Yes.
Q Do they also allow attackers to gain a sense of the architecture of the target system?
A Yes.
Q Now, SQL injection queries, can they be run with preexisting programs like SQLmap?
A Sure. There is a large amount of preprograms.
Q Is it also possible to have a SQL injection query using nothing more than a Internet browser window?

A Yes.
Q What part of the Marketwired system did they initially target with SQL injection queries?
A There was an application that we refer to as CS3 application that was used to among other things to submit press releases by, used to submit press releases for clients.
MR. TUCKER: Ms. Mulqueen, just for the witness.
COURTROOM DEPUTY: Just the witness.
Q Showing you what is marked for identification as Government's Exhibit 710. Can you see that on your screen, Mr. Gimbi?
A I can.
Q What is this document generally?
A This is an illustration of how the CS3 application and another application UK or U.S. distribute was architected. So every picture of a computer tower here represents a different machine or virtual machine. It illustrates the relationship how they work together in order to build this application, the CS3 application.
Q Does this document fairly and accurately represent a portion of Marketwired, correct?
A Yes.
Q Would that assist your testimony?
A Yes.
MR. TUCKER: We admit 710 for demonstrative

purposes.

THE COURT: For demonstrative purposes. Objections?

MR. HEALY: No objection.

MS. FELDER: No objection.

THE COURT: In evidence.

(Government Exhibit 710, was received in evidence.)

MR. TUCKER: May we publish?

Q Mr. Gimbi, can you indicate now on Government's Exhibit 710 the portions of Marketwired systems architecture that supports that CS3 application?

A On the left-hand side -- we see two boxes, one very large box and one small. On the left-hand side working from the top down we have a --

Q Sorry, if you tap on your screen it will light up.

A Excellent. So here we have what is known as an F5 load balancer, I'll come back to that in a second. Let's start with the database.

This cylinder down here represents that filing cabinet, the digital filing cabinet. That is a file that is stored redundantly on these two systems here, MW128 and MW127. Those would be referred to as the database servers, the actual physical computers that are the interacting with that database file.

Q Are those sometimes called back end servers?

A Yes.

Q What about those two servers, MW101 and MW015, how do they factor into the CS3 application?
A They are called front end servers. These are the actual web servers that are providing the user with a web experience when they request the application address.
So for instance, pretending this is Google for a second. You go to Google.com, these are the servers responding to you.
Q What is the F5 appliance?
A F5 appliance is a load balancer. So when you're talking about an application that has a lot of requests coming in, it's desirable to have redundant series of servers. So basically if something goes wrong with one server, too many requests for one to handle all of the requests, the load balancer will distribute those requests across multiple servers.
Q So the CS3 application, it's constituent parts, is that F5 load balancer, then the four servers MW10, MW15, MW128, MW127?
A That's correct.
Q Did you review the web log files for that CS3 application?
A I did.
Q Did you see indications that the attacker was using the SQL injection technique that you testified about?

A I did.

MR. TUCKER: May I show the witness, Ms. Mulqueen?

COURTROOM DEPUTY: Certainly.

Q Showing you what is marked for identification Government's Exhibit 711. Do you recognize this document, Mr. Gimbi?

A I do.

Q Is this an excerpt from the web logs for the CS3 application?

A It is.

Q Is this just a tiny excerpt of a very, very large log?

A It is.

Q Is this a fair and accurate excerpt?

A It is.

MR. TUCKER: The Government moves to admit 711 in evidence.

THE COURT: 711, any objection?

MS. BRILL: No objection.

MS. FELDER: No objection.

THE COURT: Received.

(Government Exhibit 711, was received in evidence.)

MR. TUCKER: May we publish?

THE COURT: Go ahead.

BY MR. TUCKER:

Q Mr. Gimbi, now that the jury can see, can you explain

what the significance of this web log excerpt is to you?

A Sure. So we were referring to the fact that different services keep different logs. Websites keep their own logs. A website keeping its own log, we refer to as a a web log.

Here we see three different lines of a web log text file. I know it looks like that it's just jumbled up, that's because there is not enough space.

Each line is represented with the start of, each line with an IP address in the beginning. So we see 77.123.63.15 in the beginning, that's the first line. The next line 77, that's line two. Then 178.1776.936.114 is the third line.

Q So three entries on this excerpt?

A That's correct.

Q Please continue.

A Each one of those three entries in this log represent one request coming through from a visitor to the website that the website server had to respond to.

Q What is that website is that reflected here?

A It is not reflected, I don't think, in this document itself. But it is the CS3 application. We pulled it from the CS3 front end servers.

Q Is the path here, the upper, the left-hand corner?

A Yes.

Q Tell us what you mean by path and what I mean by path?

A A path is the partial or entire, how to phrase, path to a website. If you go to, for instance sticking with Google.com, you decide you want to see what the news from Google might be, you can go to Google.com/news. The news part is the remainder of the path. Here we see again /MW/cookietext is the final part of the web address. So this would have been something along the lines of secured up Marketwired.com/cookietext. The remainder of this is also part of the path up until that point.

Q What is the significance of this highlighted text, test, what is happening?

A So again with the full path this would be at top of the URL bar in the user's browser. We see up by the cookie texting a valid request, that's just the request for a page, non-malicious part of the CS3 application. After the question mark we see manipulations from an attacker. We see HTP.print which is an oracle function. An oracle is the developer of the database that we were referring to earlier. So this is an oracle function that allows you to essentially print any designated text at the end of a specified web page.

Q Is that the HTP.print command?

A Yes.

Q What text did the user try to print with this particular HTP.print command?

A The word test. So in essence what you would get is the

expected contents of the page cookie_text, followed by "test" at the very bottom of the page, literally the four characters T-E-S-T.

Q The web page would look exactly the way Marketwired would want it to look and the word test would appear on the bottom?

A Yes.

Q What is the point of doing that?

A It's a way of validating that you found a real vulnerability.

Q That's a SQL injection of vulnerability?

A That's a SQL injection of vulnerability.

Q What is the significance of the next entry?

A Essentially the same. Let's work through from just beyond the obviously change of the text.

We notice that the IP address in the first line and second line are the same. We also notice that the string here, the user agent string, which I'll come back to is also the same.

Q User agent string?

A User agent string.

Q Continue.

A The IP address is the same, which is a strong indication that the requests came from the same machine or at least the same network. Again an IP address is essentially your address on the Internet. So two requests coming from the same IP

address is a strong indicator you may be dealing with the same or a related individual or machine making the request.

The significance of the user agent string -- I don't know if you can clear this again or for me -- the user agent string, I'll go ahead and underscore each of these. So that string, is the same for both the -- excuse me sloppy underlying -- is the same for the first log entry and the second log entry.

Q So it's clear, among other things user agent string first two entries refers to Windows NT?

A Yes, NT5.1.

Q What is a user agent string, what does to do?

A User agent string tells the web page information about your computer, about the languages that you like to use, and about the device that you're on -- excuse me, the web browser that you're using. The idea here is, if you're a web developer you can customize what gets returned to the user based on what is appropriate to them. If I have a user who speaks Italian, I want to make sure if I see indicators that they use Italian language text on the browser I will want to return them in Italian that web page. Similarly if I see -- sorry.

Q Go ahead.

A If I see that they are coming from Firefox versus Chrome, I may treat the page differently. Or if I see they are coming

from a hand-held phone versus a full-sized computer, I may serve them slightly different texts.

It's meant to be useful for developer from a forensic stand point.

It's highly likely these three requests came from the same web browser. Further cemented by the identical vulnerability and by the similarity of the time stamps.

Q So it's clear, the first two requests came from the same web browser, is that what you mean?

A Yes.

Q So it's clear, there are dates and times for these first entries the one 17 February 2010 at 1138 minus 800?

A Yes.

Q The second entry it looks like it's 14:38 this is minus 500, so it's about 17 seconds later?

A That's right.

Q If this particular SQL injection query would have run, what is the text that would appear on the bottom of the screen?

A The text would look exactly what we see here, with the exception that when text is rendered from this format there is a symbol here, the %20. %20 would render it as a space instead of percent 20.

So ultimately what this would look like is the word ya, followed by a space, followed by hacker, followed by a

space, followed by neebatso.

Q Did that same SQL injection command show up again in the web log here in the, entry which occurs about 40 seconds later at 11:39:19, on 17 February, 2010?

A Yes.

Q Forty-five seconds?

A Yes.

Q Mr. Gimbi, what is the significance of these three entries?

A Well, again, we see the first two are likely coming from the same user same browser. The last one is identical to the second request coming from at a different IP address with a different user agent string. This is a strong indicator that, very highly consistent with somebody realizing they have found a real vulnerability, customizing it in some way which is common in pen-testing hacker culture, and sharing with a second individual.

Q Just so it's clear, when you pen-testing?

A That's penetration testing. Penetration testing, the practice of hacking for a legitimate purpose, usually with a way of finding vulnerability so a company can fix them.

Q Mr. Gimbi, before any attacker could use the SQL injection queries, would they have had to log in to the CS3 application with a valid username and password?

A They would either log in or be able to create an account

with -- they would have to be able to create a valid account with a specific code.

Q The bottom line is they couldn't use these vulnerabilities without getting past that first login layer?

A That's correct.

Q So it's clear, Mr. Gimbi, this is the first indications that you saw in the CS3 web logs of malicious activity targeting Marketwired and CS3 specifically?

A First successful. There was some scanning that happened before.

Q What is scanning generally?

A Automated procedure to make sure -- not to make sure -- to see if you can identify, again low hanging fruit, low effort, high value vulnerability before you put in a manual effort to put your own hole in the system.

Q Did the web logs reflect additional SQL injection queries targeting the CS3 application after these?

A Yes.

Q What did you see?

A Two broad categories. Number one, specific queries trying to extract certain pieces of information from the database.

And then secondly, after that we saw many, many, many requests for wholesale extraction of the contents of the database press releases.

Q Just so it's clear, when you say extraction, that's taking data out of Marketwired systems?
A Correct.
Q And that extraction involved press releases?
A Correct.
Q Was also some the data that was extracted employee information from Marketwired employees?
A It was.
Q Why might a malicious cyber attacker might want to steal employer information?
A Well, the primary cause is for use for what we call escalation of privileges.
Q What is that?
A Essentially with most breaches, nearly every breach I've worked on, the attacker will get access to an employer and have some level of access. Usually the level of access the individual who they were able to hack into, whatever user that may have been. Different users of course have different levels of access. So some users may be able to access a certain set of data, some users are able to change a certain set of data, others not.

An attacker, depending on what their goals are, depending on what they are looking to accomplish, may require more access than they originally have. Stealing credentials, usernames and passwords, is the easiest way to do that.

Q In the course of your work in this engagement at Marketwired, were you provided with files that federal agents had recovered from computers overseas?
A I was.
Q What did you do with those files generally?
A I catalogued the information that was on those files and made a record of what they represented.
Q I'm going to show what you what is in evidence as Government's Exhibit 411, which is ftpusers.txt. And 444, which is employees.txt. Have you seen these documents prior to your testimony here today?
A I have.
Q Were those among the documents provided to you in the Mandiant time by federal authorities?
A They were.
Q What did you conclude about these documents, specifically Government's Exhibit 444?
A We concluded that it was highly, highly likely that they were the output of specific SQL queries that we had seen in our network. Evidence that we were able to identify Marketwired logs, mapped nearly identically to what we saw on the Secret Service disk.
Q So you were able to replicate some of those same SQL queries?
A Yes.

Q You got same the output?
A Same output. And there were other factors. The blast modified time stamps of the files matched perfectly when the requests had gone through; which is to say, they were created and manipulated at the same time that the queries were seen on the Marketwired side.
Q Showing the witness Government's Exhibit 711. There is a reference to iwire. What is that?
A In this case iwire can be the name of the account running the web service application.
Q What does that mean?
A So a web service is the software that actually sends a page back to you when you make a request. You go to Google.com, somebody sends you that logo in that back, that somebody is a programmer on a Google server somewhere. The program that's running, we call that a web server, is very similar to programs we're familiar with, Word or Solitaire or your web browser, in that there needs to be an actual user who is logged on to the computer, an account logged on to the computer to run those applications. So in this case, iwire is simply the name of the account that is running the web server application.
Q Did you see evidence that the attackers were elevating the privileges of this iwire account after these initial login entries February 2010?

A I did.
Q What is the significance of that, that elevating the privileges?
A The elevation of privileges in this case would have allowed somebody who was able to control queries from the iwire account, in this case the attacker, would be able to essentially take control of the database system. They were able to run commands as if directly from the keyboard.
Q Showing you what is in evidence, 710. Did that elevating of privileges of the iwire account allow for lateral movement within Marketwired systems?
A Yes.
Q What does that mean?
A It means that because of successful privilege escalation they were able to make modifications or changes, moved to the back end applications from the front end application, or back end servers to the front end servers.
Q They were able to increase their access to Marketwired?
A Yes.
Q And facilitate data extraction?
A Yes.
Q Did you see indications in the web logs that the attackers were successfully extracting press releases, draft press releases, from the CS3 application?
A Yes.

Q Tell the jury what you saw.
A We saw the development of five, I believe it was five, different methods for extracting press releases using this application over the course of several years. So they used different techniques, but at a rate that showed that they were automating on the back end, meaning write a program to do it for them.

So they found a technique, they would have manually figured out exactly how to get what they want and apply that into a network and do that over and over again.

Q Did you see that activity from February 10 through your arrival at Marketwired in the summer 2013?
A Yes.
Q Based on your review of web logs and the associated data, approximately how many draft press releases were the attackers able to extract from Marketwired systems during that period?
A Somewhere around the order 120,000.
Q 120,000 unique press releases?
A Right.
Q Did you see evidence that the attackers were targeting another part of Marketwired systems, that is the UK distribute server, shown here on Government's Exhibit 710?
A Yes.
Q What did you see?
A We saw attacker log into that application. And using the

access that they had from that -- from that application, manipulate the secure one server, right here, so that they could access data that was stored on the server over here.

Q A few questions about that. First, the UK distribute server, what web domain or flat fronting domain?

A USdistribute.com.

Q This was a server that made USdistribute.com work for Marketwired?

A Yes.

Q Secure one is a back end server?

A Yes.

Q You mentioned a NAS a minute ago, what is a NAS?

A NAS is network attached storage server, another term for file server. A NAS server basically allows users to place and modify files on a network while gaining access to somebody else's computer.

Q Through this of targeting the UK distribute server, the attackers were able to extract data from the NAS among other locations?

A Yes. And the NAS, again, was on the internal network.

Q Not even connected to the Internet directly?

A No.

Q You said that the attackers had to log into the USdistribute.com site, can you explain how they did that?

A There would have been a login prompt. They use the

credentials, username and password, demo and demo.
Q The username is demo and the password was demo?
A Yes.
Q That facilitated this initial entry?
A Yes.
Q Did your review of this portion of Marketwired system and the associated web logs, reflect the attackers able to install web shells?
A Yes.
Q What is a web shell?
A A web shell is a form of malware, which can have many purposes, but ultimately is just a particular way of getting a computer to do something, a script. Most often it allows attackers to run commands against the web server that they have infected.
Q If you're able to extract data using SQL injection queries, why might you use a web shell?
A Well, again, there were multiple different attempts -- or excuse me, different methods that were used, several methods to extract press releases had been cycled through and this was another one of their methods. It's also possible there were of different press releases on this web server than on the back end database.
Q Did you see other evidence that the attackers were using Marketwired login credentials to extract date from Marketwired

systems?
A Yes.
MR. TUCKER: If I could just show just the witness what is marked for identification as Government 712.
COURTROOM DEPUTY: Just the witness.
Q Do you recognize this document generally, Mr. Gimbi?
A I do.
Q What is it?
A Another web log from Marketwired application.
Q This is another excerpt from are the CS3 web logs?
A Yes.
Q This is from March 27, 2010?
A Yes.
Q Is this a fair and accurate excerpt from those web logs?
A It is.
MR. TUCKER: Move 712 into evidence.
THE COURT: 712, any objection?
MR. HEALY: No objection.
THE COURT: 712 received.
(Government Exhibit 712, was received in evidence.)
MR. TUCKER: May we publish, your Honor?
THE COURT: Go ahead.
BY MR. TUCKER:
Q Turning your attention to a few rows on this web log excerpt, Mr. Gimbi. Can you explain for the jury the

significance of these highlighted entries here DKHOO and password at password. Also this reference to rgibson@iwire.com and the password daustin8?

A These are different attempts to, requests, submitting username and password for authentication, login attempts. We can see that the requests map two different login pages, including the Mwire_login2 and just login2 by itself. There is also a NASDAQ login here. I think that was it for this case, or for this instance.

These would have been or did map, at least the rgibson and the daustin8 are credentials that were Marketwired employee credentials.

Q Did you confirm that with representatives from Marketwired during the course of the engagement?

A We did.

Q How did you determine that these were not simply Marketwired employees logging into their systems in an authorized way?

A There are a couple of factors. First, these IP addresses we see here mapped again to IP addresses we saw the attacker using earlier. Secondly, Marketwired actually went and spoke with personnel to validate whether or not they were logging into this application at these times. The personnel said that they had not.

Q On that first point. It's the same IP address that we

looked at earlier Government's Exhibit 711?

A It is.

(Continued on next page.)

Q In the course of your review of these Web logs and the other forensic analyses that you conducted, did you see evidence that the attackers were manipulating the Web logs?
A Not the Web logs, but other logs.
Q What kinds of logs did you see them manipulating?
A There was a log that the application itself -- the Marketwired developers had built into their application; and the log was not nearly as comprehensive, it didn't show area distance, but what it did show was the last time that a user would have logged into an application.
Q Did you see manipulation of those logs, those application logs?
A We did.
Q What did you see?
A I saw the attacker specifically query for specific IP addresses, so the attacker knew that they were coming from specific IP addresses and made an effort to remove any entries containing those IP address from the logs.
Q What would be the point of that?
A The point would be to, again, evade detection that a breach had happened in the first place. And then, secondly, if the breach were detected, it would cover their tracks; it would make it more difficult to investigate.
Q Did your forensic review uncover any evidence linking the malicious activity to the IP address 94.100.28.42?

A Yes.
Q What did you find specifically?
A That IP address was used for extracting press releases from the Marketwired application.
Q Was one of your objectives in responding to Marketwired to identify who the hackers were?
A No.
Q In the course of your work, did you reach any conclusions or uncover any evidence that might relate to the identities or locations of the attacker?
A The conclusions that we could come to were based off of two sources -- again, this was not a primary objective -- but first analyzing the IP addresses where all of the theft had come from, we realized that most of them had been cycled through for proxies, things like tour and other redirect methods, basically obfuscating where the requests had come from making it harder to tell exactly what server the requests had been issued from.

We did notice that an unusually high number of those IP addresses were based out of the Ukraine, but aside from that, we didn't notice any trends.

Beyond that, the other conclusion we could come to again is that whatever server or computer the Secret Service had recovered their artifacts from would have been involved in the malicious activity that we saw in Marketwired.

MR. TUCKER: Your Honor, can I have a moment to confer with my colleagues?

THE COURT: Yes.

(Short pause.)

Q Mr. Gimbi, were there subsequent teams that from Mandiant that responded to Marketwired after your work on that project completed?

A Yes.

Q Preparing for your testimony today, did you review the reports prepared by the subsequent teams?

A I did.

Q Just generally, based on your review of those reports, did you see some of the same hacking techniques being employed after you left Marketwired in the summer of 2013?

A Yes.

Q Those included SQL injection queries and the use of Web shells?

A Yes.

Q And did they also include the use of stolen login credentials from Marketwired employees?

A Yes.

Q Mr. Gimbi, even while you were at Marketwired during the summer of 2013, was Marketwired still an ongoing target of malicious cyber activity?

A They were.

MR. TUCKER: Your Honor, I have no further questions.

THE COURT: Well, I think we can all use a break right about now, so we will take our afternoon break. We will resume in about 12 minutes.

THE COURTROOM DEPUTY: All rise.

(Jury exits.)

THE COURTROOM DEPUTY: You can step down, sir.

(Witness steps down.)

THE COURT: All right.

(Witness resumes the stand.)

THE COURT: I want to talk some more at the end of the day about subject matter of our early morning discussion.

(Jury enters.)

THE COURT: Okay. Please be seated, everyone.

Before we begin the cross-examination, I want to add a little footnote to the schedule that we gave you last week, drawing your attention to Thursday, which is an unusual day, we start at one o'clock, but that's after lunch, so make sure you have some lunch beforehand, okay? We'll take a somewhat extended break in the middle of the afternoon to get you refreshed, but we will start at 1:00 and we are not going to stop for lunch, okay?

All right. Cross-examine, Mr. Healy?

CROSS-EXAMINATION

BY MR. HEALY:

Q Good afternoon, Mr. Gimbi.

A Good afternoon.

Q I just want to be clear, you and Mandiant, your company at the time, you didn't design the Marketwired system, did you?

A No.

Q And, in fact, you didn't maintain the Marketwired system prior to 2013, did you?

A No.

Q You, Mandiant -- you and Mandiant were hired in June of 2013 by Marketwired's attorneys, correct?

A Correct.

Q And that was because the Secret Service had notified them that there was a compromise in their system, correct?

A Correct.

Q And your team came in to do your incident response, correct?

A Yes.

Q And in the course of your incident response, one of the things you told the jury earlier is between the time you were called in in June going back to February of 2010, there had been evidence of hacking, correct?

A Yes.

Q About three year's period?

A And change, yes.
Q And change.
And Marketwired was unaware of this, correct, until the Secret Service informed them.
A To the best of my knowledge, yes.
Q Now, when you came in, you explained that you had a three-part objective, and one of the objectives was to prevent future intrusions, correct?
A Yes.
Q And the way you did that, for example, in this case, was you made very specific recommendations; for example, implementing keyword blocks.
A Yes.
Q And removing malicious Web shells from the server?
A Yes.
Q And disabling the accounts that you told us the hackers were using to upload those Web shells, correct?
A Yes.
Q And putting in HTTP Web log monitoring to see what was going to be happening, correct?
A Yes.
Q And implementing file integrity monitoring on some of those servers that were in the architecture trunk, correct?
A Yes.
Q And when your team finished, which I believe was on or

around June 19th of the 2013, you testified that even then there was still some evidence that Marketwired was under attack, correct?

A Yes, with the caveat of the exact finishing date, I'm not sure of, but I know that we continued to be continuously engaged through and into July.

Q Correct. And I was going to ask you, do you recall that Mandiant was hired again in July to come back to Marketwired?

A I'm aware that that happened, yes.

Q And at that time, they did a follow-up incident response.

A Yes.

Q And they found that because -- they found that because an employee reported that someone had logged into his 3 -- CS3 account and used it while he was on vacation.

A I don't recall that, but that may be in the report.

Q You don't recall.

And isn't it true that the Mandiant team found that data had been removed from the server between June 24th and July 30th?

A June 24th and July 30th of 2013?

Q Of 2013.

A I believe so. I would have to check to be absolutely sure.

Q And at the end of that process, your team, Mandiant, instituted another set of containment steps that they advised

Marketwired to take, correct?
A From the second breach?
Q Yes.
A I would presume so, but I -- again, I was not directly part of that procedure.
Q And are you aware that in November of 2013 Mandiant was called back again to Marketwired by their attorneys?
A Yes.
Q And at that time, again, an incident response was initiated.
A Correct.
Q And they did an analysis on the servers, and what they found is that again there had been an intrusion.
A Yes.
Q And they found that the intrusion, the earliest evidence of any compromise, was on November 17th of 2013.
A Okay.
Q And would you agree with me, Mr. Gimbi, that that indicates that Mandiant did their job very well, that there was no intrusion between July 30th, 2013, and October 17th of 2013?
A I'm sorry, could you rephrase the question?
Q Sure.
When Mandiant left the second time, July 30th of 2013, they had put in place recommendations to secure the

system.
A Right.
Q When they came back in November, they indeed found that there had been another intrusion, but that intrusion just started on October 17th of 2013, correct?
A From my reading of the report, I believe so, yes.
Q So that the server was secure from the date of July 30th, 2013, to October 17th of 2013.
A I would always hesitate to use that language. Frankly, most systems are simply not going to be perfectly secure, and if you're not starting from a mature standpoint already, there's always going to be holes. It's just a matter of whether or -- it's always -- there will always be holes. It's a matter of whether or not the attacker who was interested in getting into the network is aware that they are there. So I would not ever say that something was secure as a matter of fact.
Q And, in fact, my question was probably not correctly phrased. My question is: There was no evidence that there was any hacker intrusion between those two dates, July 30th, 2013, and November 17th of 2013.
A I would not be able to refer to that directly from my experience aside from what I had seen in the reports.
Q Do you recall anything that you saw in the reports that indicated anything to the contrary?

A No.
Q And then after Mandiant left in November of 2013, are you aware that they were called back again in June of 2014?
A That sounds correct.
Q And, again, they initiated the same type of incident response.
A I know there was various types of services we provided. I don't remember if that particular one was an incident response or compromised assessment.
Q Whatever we call it, are you aware that when they did their analysis, they determined that the earliest evidence of compromise was in February of 2014?
A I don't recall that.
Q Are you aware that even though if there was evidence of compromise, this time there was no evidence of any information exposure.

THE COURT: Is this something you were involved in?

THE WITNESS: No.

MR. HEALY: Your Honor, he testified that he reviewed all the subsequent reports prior to his testimony, and some of the government's questions referred to information contained in those reports.

THE COURT: All right. Go ahead.

A I'm sorry, what was the question?
Q I wondered if you were aware that when they did their

either compromise report or incident response report that they found that even though there had been some tempted intrusion that there had been no information exposure?

A That does sound familiar from the 2014 report, yes.

Q Essentially, it was still locked down from the good job that Mandiant did in November of 2013.

A Again, I would always be careful with --

Q There was no evidence --

A Yes. Yes.

Q And then they came back again in August of 2014; are you aware of that?

A Yes. I'm aware that there was another engagement in 2014.

Q And at that time, during that investigation, they did find that there was some exposure.

A Information exposure? Information theft?

Q Yes.

A I remember seeing something along those lines in the reports, yes.

Q And are you aware that the exposure was limited to the dates of July 18th, 2014, to July 22nd of 2014?

A I do not remember the specific dates.

MR. HEALY: No further questions, Your Honor.

THE COURT: All right.

Ms. Felder?

CROSS-EXAMINATION

BY MS. FELDER:

Q Mr. Gimbi, you testified that in your review, malicious activity was noted as early as February of 2010?

A Yes.

Q And your team arrived in June of 2013?

A Correct.

Q The scope of your work was not to determine who the actual actors were, correct?

A Correct.

Q The scope of your work was just to determine what type of intrusions there were --

A Right.

Q -- and how to secure the system; is that right?

A And where applicable, identify the stolen data.

Q Were there sophisticated techniques used to intrude the particular S -- CS3 application?

A It depends on how you define "sophisticated." I would say no.

THE COURT: Would I say yes?

A So one -- I'm trying to determine what kind of depth is useful here.

Q Let me give you an example.

An S Q L or SQL injection, is that considered sophisticated?

A It's not considered sophisticated, but sophisticated hackers do use it.

Q And what about malware?

A All -- most every hacker would use malware, yes.

Q But you would agree that typically average computer user would not know how to create a SQLmap or a SQL injection, correct?

A Well, most of those tools, like, when you are talking about SQLmap, are things that you can just Google and download and run, that's point click. There's very little level of sophistication that needs to go into that, and I would certainly say that most people would dabble with testing -- kind of cut their teeth and get started by downloading prebuilt tools like those.

(Continued on the following page.)

BY MS. FELDER: (Continuing.)

Q But you were hired to secure the system; correct?

A We were hired to investigate what had happened with regard to a particular breach and to provide recommendations surrounding those observations.

Q And you made those recommendations; correct?

A The head of our team was charged with drafting the specific recommendations.

Q Right, but those recommendations were implemented to secure the system?

A With mixed consistency, I believe due to technical limitations on the team. For instance, I'm aware that technical blocks around certain keywords were able to be implemented right away as soon as we requested those, but more advanced recommendations I think had taken them more time.

Q Right that's understandable. You testified you would be hesitant to every say that any system is perfectly secure; is that right?

A That's correct.

Q But there are steps that you can take to make it more secure than it was?

A That's correct.

Q Especially after you've identified the techniques used to intrude the system; correct?

A Yes.

Q Another technique used by the actors was the use of employee usernames and passwords?
A Correct.
Q And once you have those provisions you will access the system; correct?
A Assuming that the passwords had not changed or there isn't any other sort of other block prohibiting the IP address from going through, yes.
Q There's one example of an employee complaining that his credentials were used to access the CS-3 portal; correct?
A Can you rephrase the question?
Q An employee complained that his CS-3 credentials were used to access the system when he was on vacation?
A I'm not sure about a complaint, but there was a relationship where we had Marketwired personnel ask specific individuals whether or not certain logins were connected to their legitimate activity.
Q What I mean is that the company became aware that employees' credentials were being used; correct?
A Yes.
Q In an unauthorized way; correct or at least it was not used by that particular employee; correct?
A Yes.
Q So user names and passwords can be used without someone's permission or knowledge; correct?

A Yes.
Q And in this case that happened. I believe you gave the example of the username Demo and a password being used?
A Yes.
Q And that password was used to infiltrate the system?
A That password was used to access the system. I'm not sure if there's a particular definition around the word "infiltration."
Q Access the system is sufficient. So you would agree that once an actor has your e-mail, your password, they can use those credentials to access your personal system or your professional system; correct?
A They may be able to if an individual is reusing passwords.
Q Correct. As long as the password stays the same, they can use it?
A Right. And if they had used the same password on two different services, yes.
Q Right. In terms of what you testified to earlier, the actors in this particular case they used various techniques to hide their tracks; correct?
A They used at least one technique to hide their tracks.
Q What technique was that?
A They deleted log entries from the -- from an application log.

Q And you were able to determine that because you have the forensic tools to do that; correct?
A Yes. It was in the logs.
Q Thank you. No further questions.
THE COURT: Anything else?
MR. TUCKER: No, Your Honor. Thank you.
THE COURT: Thank you, sir, you may step down.
(Witness excused.)
THE COURT: Next witness, please.
MS. NESTOR: The Government calls Bret Padres.
THE COURTROOM DEPUTY: Please take the stand and raise your right hand.
(Witness sworn/affirmed.)
THE COURTROOM DEPUTY: Have a seat and state and spell your name for the record.
THE WITNESS: Bret, B-R-E-T, Padres, P-A-D-R-E-S.
(Witness takes the witness stand.)
BRET PADRES, called as a witness, having been first duly sworn/affirmed, was examined and testified as follows:
DIRECT EXAMINATION
BY MS. NESTOR:
Q Good afternoon.
A Good afternoon.
Q Where are you employed?
A The Crypsis Group.

Q What is the Crypsis Group?
A A cyber security professional services consulting firm.
Q What is your position at the Crypsis Group?
A The CEO.
Q Crypsis is C-R-Y-P-S-I-S; is that correct?
A Correct.
Q Can you tell us what your responsibilities are at Crypsis?
A In addition to being the CEO, I help run investigations. So we help people with data breaches when they believe that somebody has gained unauthorized access to their data and we can help remediate or prevent that from happening again.
Q Are you testifying here today in your capacity as the CEO of Crypsis Group?
A Yes.
Q Were you retained by the Government?
A Yes.
Q Are you testifying her today pursuant to a retention by the Government?
A Yes.
Q And are you being paid to testify here today?
A Yes.
Q How much are you being paid?
A I think to date our invoices have been somewhere in the neighborhood of $200,000.

Q When you did -- withdrawn.

When you joined Crypsis Group -- when was that, first of all.

A I joined the firm in January of 2017.

Q What did you do prior to that?

A Prior to the Crypsis Group I was at a firm called Stroz Friedberg.

Q What is Stroz Friedberg?

A Similar to the Crypsis Group it is also a cyber security professional services firm.

Q Can you tell us briefly what that means, a cyber security professional services firm?

A We are consultants that help people both proactively and reactively. Reactively meaning when people believe there's been a cyber security incident and they need help investigation what has occurred, what is the scope of what has occurred. And then proactively means before there's a cyber security incident, help prevent, help secure their network so there is not an incident; help protect from individuals gaining access to their network.

Q How long were you at Stroz?

A Close to nine years.

Q And what positions did you hold generally while there?

A While at Stroz Friedberg I was director of digital forensics, director of incident response and managing director

of cyber resilience.

Q And what were your main duties while you were at Stroz?

A Typically my main duties were to lead large investigations, to help with policies and procedures about how we help to structure and go about those investigations, hiring, mentorship and sort of build the practice of mostly incident response, data breach response.

Q Part of your duties was data breach response?

A Correct. Many of the breach responses that were performed at Stroz Friedberg during the time I was there -- well, I left.

Q What did you do before Stroz?

A I was the director of incident response at a company called Mandiant.

Q Did you have similar responsibilities there?

A Similar. Maybe the one difference being that at Mandiant I was -- it had less to do with the proactive work and it was mostly reactive work. So it was all data breach response not the proactive, help people prevent this from happening.

Q And before Mandiant where were you?

A I was at firm MZM, a firm that was acquired by Athena and I was the director of cyber operations.

Q And what did you do in that position?

A I was a contractor for the Government and we did counterintelligence operations. It was less like Stroz

Friedberg or the Crypsis Group or Mandiant. It was government work and counterintelligence.

Q What did you do before Athena?

A I was a special agent with the Office of the Inspector General at the postal service where I did investigations in computer crime.

Q Do you also have specialized training in forensics work?

A I do.

Q What is that?

A I had certification in what's known at EnCase. EnCase certification is a standard software package and standard certification for professionals in the digital forensics field. I have a reverse engineering certification and reverse engineering malware which is taking software and tearing it apart and trying to understand what its application is. I have --

Q While -- go ahead.

A And I have a certification, computer information systems security professional certification.

Q While at Stroz and currently at Crypsis Group, have you handled hundreds of investigations?

A I have, yes.

Q And have you testified in connection with your work at Crypsis Group?

A I have.

Q Have you been qualified as an expert?
A Yes.
Q An expert in computer forensic analysis?
A An expert in digital forensics, correct.
Q And while at Stroz did you also testify as an expert?
A Yes.

MS. NESTOR: Your Honor, at this time we offer Mr. Padres as a witness for information security, computer forensics and cyber incident response.

THE COURT: Any inquiry at this time.

MR. BRILL: No, Your Honor.

THE COURT: Proceed.

BY MS. NESTOR:

Q I want to turn your attention to March of 2012. Did there come a time when you were part of a Stroz team that worked on an engagement at PR Newswire?
A Yes.
Q And what was briefly what was your understanding of what events lead to that engagement?
A We were hired by PR Newswire. It's my understanding that they were approached by law enforcement with information that they may have had an intrusion into the network, that someone may have gained unauthorized access to their networks.
Q What were you hired to do by PR Newswire?
A We were hired to supplement their team and help them

investigate whether in fact there was an unauthorized access to their network and what the scope was and then assist with them providing information to law enforcement should we find information.

Q What did your team do when you were hired in March of 2012?

A Initially we responded on site to their data center and collected information from a number of their servers and began analysis to determine whether or not unauthorized access was gained to those servers or the PR Newswire environment.

Q What were your preliminary determinations?

A Fairly quickly upon initial analysis we determined that unauthorized access was gained to their environment.

Q What did you do once you determined that?

A One of the things we did was deployed a network traffic-capture device. It's something we call a sniffer. So we put this device on the network that allows us to collect network traffic and that allows us then to analyze that traffic to examine the contents of what kind of communication is going on between the PR Newswire network and other systems on the internet.

Q Generally what types of evidence did you collect when you were hired by PR Newswire in March of 2012 other than the standard information?

A We collected a number of images, meaning we copied the

system's several web serves, application servers, log server, meaning a server that collects and maintains web access logs and a file transfer server, a secure file transfer server. We made a copy of one of those as well.

Q You collected server images?

A Yes.

Q The sniffer data we discussed?

A Yes.

Q And some web access logs?

A Correct.

Q Now, did there come a time when you were retained by the Government in this case?

A Yes.

Q What were you asked to do?

A So, I was asked to take possession of a number of items that were in possession of Stroz Friedberg, examine that data, perform analysis and come to opinions with regard to the extent and method in which there was a compromise of the PR Newswire environment.

Q Did you see the data from Stroz?

A Yes.

Q What data?

A A number of the web servers, application servers, a log server and the FTP server.

Q What's an FTP server?

A FTP stand for file transfer protocol. So the FTP server is a server that is placed on the internet to allow people to transfer files to and from that server. PR Newswire needed people to transfer files to their environment and copy files from their environment and to do so they used this server called FTP server.

Q Did you prepare any reports summarizing your findings in the course of this engagement?

A Yes.

Q Would those assist you in your testimony today?

A Yes.

Q And did you prepare reports during your time at Stroz as well?

A I did.

Q And would those help you in your testimony today?

A Yes.

MS. NESTOR: With the Court's permission, I'd like to hand the witness 3500-BP-1 and 3500-BP-2.

THE COURT: Okay. BP-1 and 2.

MS. NESTOR: Your Honor, I'm handing up a binder of exhibits which I will mark for evidentiary purposes in a few moments.

BY MS. NESTOR:

Q Generally did you see evidence of malicious activity on the PR Newswire servers in your most recent review after you

were retained by the Government?
A Yes.
Q What were your findings?
A I found that as early as April of 2010 that there was unauthorized access gained to the PR Newswire network.
Q And, to be clear, the servers that you testified that you received from Stroz and reviewed, what was the time span of those servers? Are you referring to your materials, 3500-BP-1?
A I am. So, these were servers that we made copies of in March of 2012 so they would have contained data up to March of 2012.
Q Now, would they have been up to March of 2012 or they're decommissioned servers that were taken offline earlier?
A It is my understanding that they were taken offline prior to that time period.
Q Now, in your experience -- withdrawn.
When you said that you found malicious activity on PR Newswire's servers, can you be mere specific about what you found?
A Sure. There was back door malicious programs, back door malicious programs placed on the server that allowed individuals to bypass normal authentication methods and have access to the servers without having to authenticate or log into those servers directly.

Q What do you mean by back door?
A So, normally you might log into a system and be presented with a prompt asking for a username and password and have to provide valid username and password credentials. If you place a back door on a system and get it to run, then you access that back door, you can bypass that normal authentication then.
Q Were you able to determine whether the individuals that were accessing or compromising PR Newswire used measures to conceal their malicious activity?
A Yes.
Q Tell us about that.
A So, they were able to install applications on the system that allowed them to remove log data and hide their activities.
Q Were you able to determine how the hackers gained access to PR Newswire's computer system initially?
A So, I was able to see that -- in this April of 2010 time frame that there was an exploit launched against the web servers but the specific exploit that gave them access to the environment, I was unable to determine that and I believe that's because the log entries that would have given me that information were missing and they were deleted.
Q Were you able to determine how the intruders actually maintained access to the PR Newswire system after they gained

access, after the initial intrusion?

A In addition to the web-based back doors that were found on the system, we found that they replaced the -- one of these -- there's a program on these systems called SSH. It's a shell program that people use to log into these servers. They had replaced the normal program with a trojanized version of this program that had additional functionality and instead of just logging the person in as normal, it also then sent a copy of that individual's credentials out of the network to the attacker.

Q Why would a malicious cyber actor want to steal employee information and login credentials in this way?

A It would allow that person to gain access to other systems. It would also allow that person to maintain access to the systems if, in fact, somebody did discover their back door and removed those back doors they would have these valid credentials that they can use to get back into the network.

Q Now, you previously testified in March of 2012 you were retained -- while you were at Stroz you were retained by PR Newswire and you installed the sniffer. Did the sniffer alert you of anything?

A Yes. In fact, that's how we initially found these credentials being sent outside the network. We were looking at the sniffer data we saw what we thought was unusual traffic. We discovered where it was coming from on several

systems. We investigated it further and found this trojanized SSH process. Upon further investigation we found that it had this functionality of sending these credentials out. They were encoded so we couldn't initially see them. And that's what sort of led us -- the sniffer data is what led us to discover this SSH program sending out this data.

Q Did you determine where the credentials were being sent?

A A number of locations. I can remember the Ukraine was one of the IP addresses that the data was being sent to.

Q So you were able to determine where the data was being sent based on the IP address?

A Correct.

Q Does that mean that in March of 2012 when you were doing your work for PR Newswire you saw evidence of intrusion through the sniffer itself?

A Yes.

Q Were you able to determine whether the malicious intruders were able to extricate press releases from the PR Newswire's servers?

A Yes.

Q Would you tell us what were able to learn about that?

A There were scripts installed on the application server that were designed to query the database, the news release database, for news release data, copy that data from the database onto the application server in a temp directory and

then send the data to the attacker and then delete that data from the application server.

Q Was the data always deleted?

A It was designed to be deleted. There were some cases in which the data still remained in the temp directory and in looking at the logs of the script writing we can see that in some cases the files that were being deleted were, like, locked and couldn't be deleted. So in 29 cases, there were 29 files still in that temp directly and those files were still there.

Q Were you able to determine how many press releases approximately there were attempts to extricate?

A Let me see here.

Q Are still referring to 3500-BP-1?

A Yes. So, because I was able to find these scrips that were designed to copy the data from the database, I also retrieved logs that showed access to those scrips. By looking at those logs I found 43,527 times in which those scrips were called to retrieve press release data from the database.

Q During what period of time?

A Between July of 2010 and January of 2011.

Q Now, you referenced that there were 29 files that were not deleted from the temp files; is that right?

A There were 29 files still in the temp directory when we created an image of that system, correct.

Q What were those files?
A They were press release data. So some of them looked to be press releases. Other files just related to press releases.
MS. NESTOR: I want to show the witness for identification only and I can do this -- I was hoping I can do this through the binder the witness has Government Exhibit 500 through 5026 and 5028 and 5029.
Q Do you recognize all of these exhibits?
A Yes.
Q What do you recognize them to be?
A These are the files that were in the temp directly on the application server.
Q Did you review them?
A Yes.
Q Are they in substantially the same condition as when you provided them to the Government?
A Yes.
MS. NESTOR: Your Honor, at this time the Government seeks to admit Government Exhibit 5001 through 5026 and 5028 and 5029.
THE COURT: Any objection, folks.
MR. BRILL: No objection, Your Honor.
THE COURT: Received in evidence.
(Government Exhibits 5001 through 5026 and 5028 and

5029 received in evidence.)

Q I'm going to publish 5002 to the jury. Can you tell us what this is that we're looking at?

A This is a press release from ACTS Retirement and Life Communities.

Q This is one of the press releases that you recovered from the server?

A Correct.

Q And what is this?

A A general dynamics press release. General dynamics is awarded 19 million for Saudi Bank Corp.

Q And that is Government's Exhibit 5002. And there are -- as you testified, there are about 29 files. Were all of them press releases?

A No.

Q Were most of them press releases?

A Correct, yes.

Q Now, you previously testified that you were engaged by PR Newswire in March. Were you retained by PR Newswire at any other point in time?

A In February of 2013.

Q Tell us why.

A They had experienced some difficulty with their file transfer server. Their SFTP server had been crashing and they were asking for help looking into the cause.

Q What is the SFTP server?
A This is the server we were talking about earlier. So it's the file transfer, the secured file transfer server.
Q Did you review the SFTP server as part of your work in that case?
A Yes.
Q And what did you determine?
A It looks as if somebody had gained access to that server and was attempting to install a -- an exploit and it wasn't working correctly and causing the server to crash.
Q What did you observe about the intruder's activity on the PR's server?
A In addition to finding that somebody had gained access and was trying to install this exploit kit to maintain access to the server, we were trying to determine how they even got onto this file transfer server to do that in the first place. It was behind what's known as the VPN. They would have had reversed into the network and they would have done it through a VPN connection. A VPN connection is a way that they can come from outside the network into the network and they were using an employee's credentials to do this.

We had suspected that what they might have done is phished or spear phished that employee's credentials and that they were using those credentials to get into the network and then hop over to the FTP server.

So we took possession of that employee's computer to do analysis of whether or not there was a malware running on that system or if we could find evidence that they were spear phishing that computer's credentials.

Q What is spear phishing?

A So, phishing is when somebody sends you an e-mail to try to get you to try to click on a link or run a program or trick you into typing if your credentials so somebody can steal those or use those credentials to gain access to the network. Spear phishing is a modification of that which it's more targeted rather than widespread to anybody.

Q And you saw evidence of spear phishing during that time?

A We did find evidence of spear phishing on that employee's computer; correct.

Q What happened after you were able to review that employee's computer?

A During that analysis we were told that they had changed the credentials, the password, for that employee and then we needed that. The access continued, but just under a different username. So the attacker switched to a different user on the VPN connection. We then started to take steps to obtain access to that user's laptop to perform analysis of that system. They changed those credentials. The attacker switched to another account and this continued which led us to the conclusion that the attacker had access to a large cache

of credentials for the PR Newswire in this environment.

Q Now, I just want to explain to the jury, what was -- back in March of 2012 and in February of 2013, what was your role in terms of what you were supposed to be doing at PR Newswire?

A We were assisting the PR Newswire staff in investigating this.

Q What does that mean, you were assisting?

A So it was really was their investigation and they would ask us for assistance and look at a particular system or help answer a specific question. There are certain clients of ours where they hand us the entire investigation. They were running it. We were just assisting.

Q Thank you.

MS. NESTOR: No further questions, Your Honor.

THE COURT: Okay.

Any questions?

MR. BRILL: Yes.

(Continued on the following page.)

CROSS-EXAMINATION

BY MR. HEALY:

Q Good afternoon, Mr. Padres.

A Good afternoon.

Q You told us in 2012 you were, working for Stroz Friedberg, correct?

A Correct.

Q And there came a time when PR Newswire engaged that firm to, I think the word you used was, assist their staff in an investigation; is that fair to say.

A Correct.

Q Based on information that they obtained from the Secret Service, correct?

A I don't recall where they specifically. I think they were working with a couple different agencies, SECE, I think the FBI. I don't recall specifically the Secret Service at that time, but maybe.

Q Let me ask it a different way. Did they engage Stroz Friedberg because some investigative branch of the Government had indicated to them that their servers had been compromised?

A My understanding is they were given information from the Government about a compromise that led them to start an investigation, if that answers your question.

Q Sounds like the answer was, yes. Thank you.

You said that your job, was your team's job, was to

investigate whether or not there was access, correct?
A Whether or not unauthorized access was gained, correct, yes.
Q And to determine if possible who was accessing the system?
A We were not engaged to determine who.
Q What was your second goal?
A Scope of compromise.
Q Scope of compromise. But you weren't engaged to try to prevent future compromise; is that fair to say?
A I'm sorry, your question?
Q Sure. Stroz Friedberg, for whom you were working, wasn't engaged to try to prevent future compromise?
A No, we were not engaged to.
Q You and your company did not design that system, correct?
A Correct.
Q You didn't maintain that system, correct?
A Correct.
Q Would you agree with me that there are certain steps that companies can take to secure their data?
A Sure.
Q Would you agree with me that one of the simplest ways would be to make sure that all security updates and patches are installed?
A If you're asking me if all security patches are installed

would it prevent all security breaches, then I would disagree, but certainly.

Q That wasn't my question. My question was, isn't that one of the simplest ways to help prevent unauthorized access to a system?

A It is certainly something we recommend, yes.

Q Sure. Is it fair to say that that's relatively simple to do?

A No, but it is certainly something that we recommend. Installing security patches can be fairly complicated, can break things. It's something that sometimes people can't update their systems, so they have to do this process we call putting in mitigating controls, but.

Q Would you agree with me, sir, that if PR Newswire was running an operating system that had been released in 2003 and they had never installed a single patch or security update, that would be evidence of perhaps a lack of diligence?

A I don't know what other controls they would have put around. We didn't look at that.

Q I didn't ask if you looked at it. I asked if they failed to did any security patches or updates from 2003 until you walked through the door in 2012, would that indicate a lack of diligence?

A That alone wouldn't.

Q So you think that would be okay?

A That alone wouldn't be enough.
Q My question wasn't whether that alone, just whether a failure to do that, sir?
MS. NESTOR: Objection, your Honor.
THE COURT: In effect it is. Next question.
Q When you did your analysis and found that the system had been compromised, I believe you said as early as 2010, correct?
A Correct, yes.
Q And then I believe you said that through that time through, January of 2011 there had been 43,000 requests for press releases; is that correct?
A Press release data exactly.
Q But that doesn't mean that they accessed 43,000 press releases, correct?
A No.
Q Would there -- in your review in your report were there evidence of requests for press release data after January of 2011?
A If I could review my -- the log data I had only went to January 2011.
Q So your review essentially says that after January 2011 you have no evidence of, because of the log data you had, any evidence of press release requests after that date?
A My review would not have that, correct.

Q You said that Stroz Friedberg was called back again in 2013?
A Correct.
Q That was because the system was crashing?
A Correct.
Q I think you told the jury that the reason the system was crashing is that people were making attempts to get in, essentially in layman's terms?
A They were already on the system, but they were trying to elevate their privileges by installing this exploit kit that I believe was causing instability and the crashing.
Q Is it fair to say they were not able, since you use the language that you did, that they were not able to install it?
A Correct.
Q Following the time that you finished, you and Stroz Friedberg, finished your work in 2013, were you satisfied at that point that your team had done what they could to assist PR Newswire in making that system safe?
A I don't think that was our role to assist PR Newswire in making the system safe.
Q Well, you said that you were there to assist them. And that your role -- is it your testimony that they weren't interested in making their system safe?
MS. NESTOR: Objection, your Honor.
THE COURT: I don't think he testified to that. I

think he testified what his role was. Find the problem, right.

THE WITNESS: Investigate, correct.

Q You made no recommendations how to solve that problem?

A We were not tasked with coming up with remediation plans for their network.

Q That would be no then, no suggestions?

A I think it would be untruthful for me to say never a time that I ever gave them a suggestion.

Q To your knowledge, well, strike that.

Were you or Stroz Friedberg ever called back again to PR Newswire to assist their team?

A After February 2013?

Q That's correct.

A There were probably times where we did interact with them, I don't recall specific dates but I believe so.

Q When you say interact, were you called back to assist them in investigation?

A So there was a time just prior to being hired by the Government, where Stroz Friedberg was asked to assist the Government prior to me being retained as a Crypsis Group employee, so there is that time.

Q I'm confused for a moment. Stroz Friedberg was asked by the Government to assist or asked by PR Newswire to assist?

A You're right, asked by PR Newswire to assist.

Q That was prior to 2017, do I have that correct?
A That would have been in 2017, correct.
Q Do you have any knowledge of that investigation?
A It wasn't an investigation.
Q Help me out, what were they asked to do?
A I believe it was to, certainly to produce data to the Government, that was one thing.
Q That's the data you reviewed?
A It includes the data I reviewed, correct.
Q Was there other data you didn't review that was produced to the Government?
A I don't know.
Q Why would you -- strike that.

Let's talk about a little about those press releases that you found in 2013. Do I have that correct, the 28 in the temporary folder?

A I'm sorry? You kind of mixed two things together.
Q Sure. Did you find when you came back in 2013, press releases in a folder that you referred to as a temporary folder?
A I didn't find that in 2013.
Q You found that in 2012?
A Correct.
Q You can refer to your binder. This is marked 5001?

THE COURT: In evidence, yes.

Q Can you look at the title of that press release, can you read that to the jury?
A New website offers up to $100 discount on Apple iPads.
Q I'm going to show you in your binder also in evidence number 5023, can you read that headline?
A National eagles and angles association will host national launch on 2011 -- January 11, 2011 in New York City.
Q I'd like you to refer to what is in evidence as Exhibit 5026. Can you read that to the jury?
A United States Mint to launch the 2011 Native American $1 coin in Plymouth, Massachusetts.
Q Finally, can you turn to what in evidence as 5017, do you see -- I'm not going to ask you to read the headline because I'm not sure there is a headline. That is what you recovered from the temporary folder?
A It is.
Q Would you agree with me none of these four documents have anything to do with earnings?
A It certainly looks like 5017, it would be hard for me to imagine it has nothing to do with earnings on the face of it. The others --
Q United States Mint to launch the 2011 Native American coin?
A Certainly based off of the headlines I just read. I would have to read the rest of them to give you an answer

about the contents.

Q Finally, would you agree with me, as you told us earlier, since there is no evidence that was obtained in 2011 because of the logs you were provided, that there was any requests for press releases after January 11, 2011, that the date of all 28 of those documents are January 11, 2011 or prior?

A Can you repeat the question?

Q Sure. You told us earlier that there is no evidence that you uncovered in 2012 with Stroz Friedberg that there were any requests for press releases after January of 2011. These press releases that were found in the temporary folder, you can certainly look through them all if you'd like, these press releases are all dated prior to January 11, 2011?

A That's my recollection, correct.

MR. HEALY: No further questions.

THE COURT: Ms. Felder.

MS. FELDER: No questions.

THE COURT: Any further questions of the witness?

MS. NESTOR: No, your Honor. Thank you.

THE COURT: All right, sir. Thank you very much. You may step down.

(Whereupon, the witness was excused.)

THE COURT: We'll call it a day, folks. We will resume at 9:30 a.m. tomorrow morning.

Let me repeat my usual admonitions with a little

emphasis, don't discuss this case, folks. When I say don't discuss the case, I don't only mean don't discuss the case and the testimony, I don't want you talking about anything about the case. In other words, when you walk out this door the case doesn't exist. All right. The time of day other than what day you start tomorrow. Please, folks. Because you know, an innocent little comment about something is liable to trigger something else. And like a house of cards, it's big trouble. So please no discussion, whatsoever.

Again, you'll pardon my tone, but we're all vested in this case, a lot of time has been spent, a lot of effort, we don't want to jeopardize that. Have a pleasant evening. Get some rest. We'll see you at 9:30 in the morning.

COURTROOM DEPUTY: All rise.

(Jury exits the courtroom.)

THE COURT: Have a seat folks. Counsel come up to the bench.

A couple of things, I haven't really had much of an opportunity trying to pay attention to what is going on to review this testimony from last week, but I will do so over the evening break. I didn't get Mr. Brill, who did stand this morning, an opportunity to speak, nor did I give the Government a chance to.

MR. BRILL: I'll defer to Ms. Brill to give our position.

MS. BRILL: Our position at this time is the same as the position of the federal public defender. We are at this time requesting at a minimum the strong curative instruction that Ms. Whalen has put forth. But that is our position now. We certainly understand that the Court hasn't completed its review. We've only begun to also absorb the contents of the Government's disclosures.

And so, but you asked for the position. That was going to be the position. That's the position we put in the morning. This is a fluid situation. We may have more to say once the Court makes a ruling.

THE COURT: You want to add anything?

MR. TUCKER: No, your Honor. Simply to say that the reason that Igor Dubovoy was brought back in was specifically was to ascertain the scope of the conduct. The Government has reviewed his testimony. It's the Government's view that in his testimony he admitted to the conduct that defense counsel elicited. The Government standing here today has no reason to believe that Igor Dubovoy perjured himself during the testimony. That's the whole reason we brought him back.

Finally, we disclosed what we learned as soon as we learned it.

THE COURT: Let me review the testimony. Look, obviously this technical aspect of this case we heard all about all day long, I know their arguments are going to be

made, perhaps there should be some dents in the Government's presentation that the defense can exploit, that's your job. But ultimately I think it's critical, it's the testimony of two or three individuals which is very important. So I take this very seriously, very seriously, which is why I want to read specifically the testimony. I do recall Igor admitting preparation of two or three documents.

I'm not as concerned about the points. Stressed somewhat a letter, it's going be apparent a disagreement between father and son as to whether or not the preparation of those documents was ordered as opposed to just done by the son who informed his father. There is a lot of room for misinterpretation and so forth. It doesn't seem to be as black and white as it's been portrayed. It's a serious matter.

That said, I don't see any authority, nor so for frankly Ms. Whalen, despite the passionate plea, do I see justification or authority for the relief you seek, either the instruction to the jury or for that matter the striking not only of the witness who we heard from, the witness we haven't heard from. That's not a final ruling.

I just wanted to say one other thing. I know this is a complicated case from everybody's perspective. I'm absorbing all this information. I don't envy the charge of the responsibility of the getting the situation to the

defense, the defense digesting it all. I seem to detect a level of rancor and it's distressing me. When you're under pressure and you don't get things when you want to get them, I fully understand the human reaction to that. But I hope we can turn the page here.

But in the process, I call upon the Government. You've got to be Cesar's wife here. The folks here are under enormous pressure dealing with voluminous information.

One area specifically of inquiry, then I'll let you go, the Latvia situation troubles me. We had motion in limine to preclude any examination. Ms. Whalen in her letter asked the question what was done here. If it's simply a question of asking the witness is there an investigation going, did you do it, yes. There is an investigation, no, I didn't do it, leaving it at that. Or did the Government take the initiative, as I think you would, to get the bottom of it and explore what sources of information are available to you. So we know what exactly is going on. We know the level of falsity, if any, in the witness's claims of not being criminally culpable.

I read the Latvian document. It was difficult to read, but one thing is clear, very specific term, a wholesale fraud. The fact that they lost $100,000 in it doesn't tell me anything. If the fraud was going to net them 5 million, what does the down payment of $100,000 mean?

I just I want to know that you've done your homework on this Latvia thing that you shared it with counsel. This goes right to the heart of this case. Is the jury going to believe these people? I assume you're going to do everything you can to pull all this technical stuff together, that's your job. I don't want loose ends when it comes to credibility, or short cuts. I don't care whether the witness has already testified, if something was said that relates to the issue of credibility, you walk a higher rope, or least you should be. I trust you're making your efforts to the do that.

That's what bothers me more than anything else, what is between the lines here. I know most of you, certainly I know Milly Whalen longer than she would like to admit. I don't want to see the woman as upset as she was. I thought I'd share that with you.

I'll review the testimony and have some rulings, if you will.

One other thing, if I turn you down on these requests to strike or to instruct the jury on so-called curative instruction, if you want this fellow back, or maybe if you're undecided whether you want him back, tell them now and we can get him back here forthwith. Same thing with Ms. Pierce, although I think that is obviously less of a concern.

MS. WHALEN: With respect to Mr. Dubovoy, our

position is not to call him back. I don't trust him.

MS. BRILL: With respect to Mr. Korchevsky, we are undecided. Awaiting the Court's --

THE COURT: I don't want to delay.

MS. BRILL: The undecided, your Honor, and I don't mean to sound like you gave a technical way out and I took it. We are planning to going back and come to a final conclusion about that. I can't say if we are in agreement or not with that.

THE COURT: I just don't want a delay here.

MS. BRILL: That is why if the Court is asking for that reason, then in abundance of caution, the Court should read between the lines. The Government should read between the lines.

THE COURT: I want this done right. If you're going to convict these people, you're going to do it right.

MR. TUCKER: The Government would make arrangements to bring Igor Dubovoy back in the city to be called quickly. The Government's understands the Court's admonition.

THE COURT: Have a good night.

(Proceedings adjourned to resume on June 19, 2019 at 9:30 a.m.)

I N D E X

I N D E X

EXHIBITS